



프라이빗 클라우드에서 **Threat Defense Virtual** 클러스터링

클러스터링을 사용하면 여러 개의 threat defense virtual을 하나의 논리적 디바이스로 그룹화할 수 있습니다. 클러스터는 처리량 증대 및 여러 디바이스의 이중화라는 목표를 달성하는 동시에 단일 디바이스(관리, 네트워크에 통합)의 모든 편의성을 제공합니다. VMware 및 KVM을 사용하여 프라이빗 클라우드에서 threat defense virtual 클러스터를 구축할 수 있습니다. 라우팅 방화벽 모드만 지원됩니다.



참고 클러스터링을 사용할 경우 일부 기능이 지원되지 않습니다. [지원되지 않는 기능 및 클러스터링, 36 페이지](#)의 내용을 참조하십시오.

- [프라이빗 클라우드의 Threat Defense 가상 클러스터링 정보, 1 페이지](#)
- [Threat Defense 가상 클러스터링용 라이선스, 5 페이지](#)
- [Threat Defense 가상 클러스터링의 요구 사항 및 사전 요건, 6 페이지](#)
- [Threat Defense 가상 클러스터링에 대한 지침, 7 페이지](#)
- [Threat Defense 가상 클러스터링 구성, 8 페이지](#)
- [클러스터 노드 관리, 21 페이지](#)
- [클러스터 모니터링, 31 페이지](#)
- [클러스터링에 대한 참조, 36 페이지](#)
- [프라이빗 클라우드의 Threat Defense 가상 클러스터링 기록, 49 페이지](#)

프라이빗 클라우드의 **Threat Defense** 가상 클러스터링 정보

이 섹션에서는 클러스터링 아키텍처 및 이러한 아키텍처의 작동 방식에 대해 설명합니다.

클러스터를 네트워크에 맞게 활용하는 방법

클러스터는 하나의 디바이스로 작동하는 여러 개의 방화벽으로 구성됩니다. 클러스터로 작동하려면 방화벽에는 다음과 같은 인프라가 필요합니다.

- VXLAN 인터페이스를 사용하는 클러스터 내 통신을 위한 격리된 네트워크(클러스터 제어 링크라고 함). 레이어 3 물리적 네트워크를 통해 레이어 2 가상 네트워크 역할을 하는 VXLAN은 클러스터 제어 링크를 통해 위협 대응 가상에서 브로드캐스트/멀티캐스트 메시지를 전송하도록 합니다.
- 구성 및 모니터링을 지원하는 각 방화벽에 대한 관리 액세스 위협 대응 가상 구축에는 클러스터 노드를 관리하는 데 사용할 Management 0/0 인터페이스가 포함됩니다.

네트워크에 클러스터를 배치할 경우, 업스트림 및 다운스트림 라우터에서는 레이어 3 개별 인터페이스와 다음 중 한 가지 방법을 사용하여 클러스터로 들어오고 나가는 데이터의 로드 밸런싱을 수행할 수 있어야 합니다.

- 정책 기반 라우팅 - 업스트림 및 다운스트림 라우터에서는 경로 맵 및 ACL을 사용하여 유닛 간의 로드 밸런싱을 수행합니다.
- Equal-Cost Multi-Path 라우팅 — 업스트림 및 다운스트림 라우터에서는 Equal Cost 고정 또는 동적 라우팅을 사용하여 노드 간의 로드 밸런싱을 수행합니다.



참고 레이어 2 Spanned EtherChannel은 지원되지 않습니다.

제어 및 데이터 노드 역할

클러스터의 멤버 중 하나는 제어 노드입니다. 여러 클러스터 노드가 동시에 온라인 상태가 되면의 우선 순위 설정에 따라 제어 노드가 결정됩니다. 우선 순위는 1에서 100까지 1이 가장 높은 우선 순위입니다. 다른 모든 멤버는 데이터 노드입니다. 클러스터를 처음 생성할 때 제어 노드가 될 노드를 지정하면 클러스터에 추가된 첫 번째 노드이기 때문에 제어 노드가 됩니다.

클러스터의 모든 노드에서는 동일한 구성을 공유합니다. 처음에 제어 노드로 지정하는 노드는 클러스터에 참가할 때 데이터 노드의 구성을 덮어쓰므로 클러스터를 구성하기 전에 제어 노드에서 초기 구성만 수행하면 됩니다.

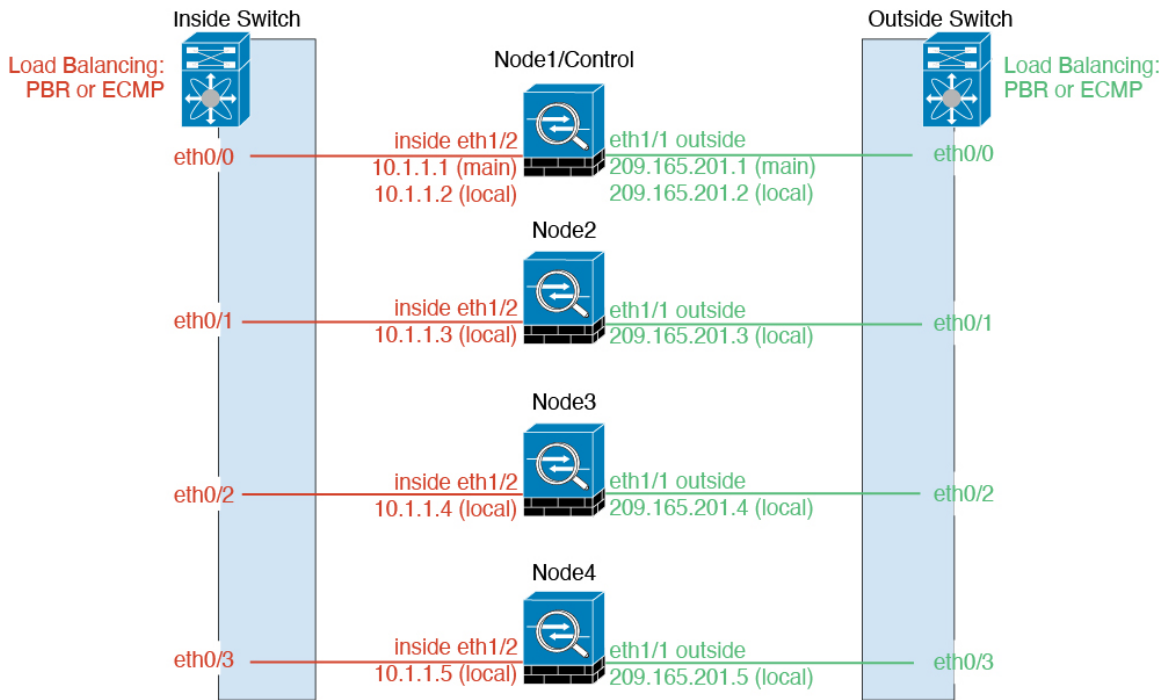
일부 기능은 클러스터로 확장되지 않으며, 제어 노드에서 이러한 기능에 대한 모든 트래픽을 처리합니다.

개별 인터페이스

클러스터 인터페이스를 개별 인터페이스로 구성할 수 있습니다.

개별 인터페이스는 정상적인 라우팅 인터페이스로, 각각 로컬 IP 주소가 있습니다. 인터페이스 구성은 제어 노드에서만 구성해야 하므로, 인터페이스 구성을 사용하면 제어 노드 중 하나를 포함하여 클러스터 노드에 대해 지정된 인터페이스에 사용할 IP 주소 풀을 설정할 수 있습니다. 기본 클러스터 IP 주소는 현재 제어 노드에 항상 속해 있는 클러스터의 고정 주소입니다. 로컬 IP 주소는 항상 라우팅을 위한 제어 노드 주소입니다. 기본 클러스터 IP 주소에서는 주소에 대한 일관된 관리 액세스를 제공합니다. 제어 노드가 변경될 경우 기본 클러스터 IP 주소는 새 제어 노드로 이동되므로 클러스터는 지속

적으로 원활하게 관리됩니다. 그러나 이 경우 로드 밸런싱은 업스트림 스위치에서 별도로 구성해야 합니다.



참고 레이어 2 Spanned EtherChannel은 지원되지 않습니다.

정책 기반 라우팅

개별 인터페이스를 사용할 경우, 각각의 threat defense 인터페이스에서는 자신의 IP 주소 및 MAC 주소를 계속 사용합니다. 로드 밸런싱 방법 중 하나는 PBR(Policy-Based Routing)입니다.

이미 PBR을 사용 중이고 기존 인프라를 활용하려는 경우 이 방법을 권장합니다.

PBR 방법의 경우 경로 맵 및 ACL을 기준으로 라우팅을 결정합니다. 클러스터에 있는 모든 threat defense 간의 트래픽을 수동으로 나누어야 합니다. PBR은 고정이므로 매번 최적의 로드 밸런싱 결과를 달성할 수 있는 것은 아닙니다. 최상의 성능을 실현하려면 연결의 전달 및 반환 패킷이 동일한 threat defense에 전달되도록 PBR 정책을 구성하는 것이 좋습니다. 예를 들어, Cisco 라우터가 있는 경우 Cisco IOS PBR with Object Tracking을 사용하여 이중화를 구현할 수 있습니다. Cisco IOS Object Tracking에서는 ICMP Ping을 사용하여 각각의 threat defense를 모니터링합니다. 그런 다음 특정 threat defense의 도달 범위를 기준으로 경로 맵을 사용하거나 사용하지 않도록 설정할 수 있습니다. 자세한 내용은 다음 URL을 참조하십시오.

<http://www.cisco.com/c/en/us/solutions/data-center-virtualization/intelligent-traffic-director/index.html>

http://www.cisco.com/en/US/products/ps6599/products_white_paper09186a00800a4409.shtml

Equal-Cost Multi-Path 라우팅

개별 인터페이스를 사용할 경우, 각각의 threat defense 인터페이스에서는 자신의 IP 주소 및 MAC 주소를 계속 사용합니다. 로드 밸런싱 방법 중 하나는 ECMP(Equal-Cost Multi-Path) 라우팅입니다.

이미 ECMP를 사용 중이고 기존 인프라를 활용하려는 경우 이 방법을 권장합니다.

ECMP 라우팅을 사용하면 라우팅 메트릭에서 가장 순위가 높은 여러 가지 "최상의 경로"를 통해 패킷을 전달할 수 있습니다. EtherChannel과 마찬가지로, 소스와 목적지 IP 주소 및/또는 소스와 목적지 포트의 해시를 사용하여 다음 홉 중 하나로 패킷을 보낼 수 있습니다. ECMP 라우팅을 위한 고정 경로를 사용할 경우, threat defense 오류가 발생하면 문제를 초래할 수 있습니다. 경로는 계속 사용할 수 있으며 오류가 발생한 threat defense에 대한 트래픽은 손실됩니다. 고정 경로를 사용할 경우 Object Tracking 같은 고정 경로 모니터링 기능을 사용할 수 있는지 확인하십시오. 동적 라우팅 프로토콜을 사용하여 경로를 추가 및 제거하는 것이 좋으며, 이 경우 동적 라우팅에 참여하도록 각 threat defense를 구성해야 합니다.

클러스터 제어 링크

각 노드는 클러스터 제어 링크에 대한 하나의 인터페이스를 VTEP(VXLAN) 전용 인터페이스로 사용해야 합니다. VXLAN에 대한 자세한 내용은 [VXLAN 인터페이스 구성](#) 섹션을 참조하십시오.

VXLAN 터널 엔드포인트

VXLAN 터널 엔드포인트(VTEP) 디바이스는 VXLAN 캡슐화 및 역캡슐화를 수행합니다. 각 VTEP에는 2개의 인터페이스 유형이 있습니다. VNI(VXLAN 네트워크 식별자) 인터페이스라고 하는 하나 이상의 가상 인터페이스에는 VTEP 소스 인터페이스라고 하는 일반 인터페이스는 VTEP 사이에서 VNI 인터페이스를 터널링합니다. VTEP 소스 인터페이스는 VTEP대 VTEP 통신을 위해 전송 IP 네트워크에 연결됩니다.

VTEP 소스 인터페이스

VTEP 소스 인터페이스는 VNI 인터페이스를 연결하려는 위협 대응 가상 일반 인터페이스입니다. 클러스터 제어 링크 역할을 하도록 하나의 VTEP 소스 인터페이스를 구성할 수 있습니다. 소스 인터페이스는 클러스터 제어 링크용으로만 예약되어 있습니다. 각 VTEP 소스 인터페이스는 동일한 서브넷에 IP 주소가 있습니다. 이 서브넷은 모든 다른 트래픽과 분리되어 있어야 하며, 클러스터 제어 링크 인터페이스만 포함해야 합니다.

VNI 인터페이스

VNI 인터페이스는 VLAN 인터페이스와 유사합니다. 이 인터페이스는 태그 지정을 사용하여 지정된 물리적 인터페이스에서 네트워크 트래픽을 분리하여 유지하는 가상 인터페이스입니다. 하나의 VNI 인터페이스만 구성할 수 있습니다. 각 VNI 인터페이스는 동일한 서브넷에 IP 주소가 있습니다.

피어 VTEP

단일 VTEP 피어를 허용하는 데이터 인터페이스용 일반 VXLAN과 달리 위협 대응 가상 클러스터링에서는 여러 피어를 구성할 수 있습니다.

클러스터 제어 링크 트래픽 개요

클러스터 제어 링크 트래픽에는 제어 및 데이터 트래픽이 모두 포함됩니다.

제어 트래픽에는 다음 사항이 해당됩니다.

- 제어 노드 선택.
- 구성 복제
- 상태 모니터링

데이터 트래픽에는 다음 사항이 해당됩니다.

- 상태 복제
- 연결 소유권 쿼리 및 데이터 패킷 전송

구성 복제

클러스터의 모든 노드에서는 단일 구성을 공유합니다. 제어 노드에서는 구성만 변경할 수 있으며(부트스트랩 구성 예외), 변경 사항은 클러스터의 모든 다른 노드에 자동으로 동기화됩니다.

관리 네트워크

관리 인터페이스를 사용하여 각 노드를 관리해야 합니다. 데이터 인터페이스에서의 관리는 클러스터링에서 지원되지 않습니다.

Threat Defense 가상 클러스터링용 라이선스

각 threat defense virtual 클러스터 노드에는 동일한 성능 계층 라이선스가 필요합니다. 모든 멤버에 대해 동일한 수의 CPU 및 메모리를 사용하는 것이 좋습니다. 그렇지 않으면 성능이 가장 낮은 멤버와 일치하도록 모든 노드에서 제한됩니다. 처리량 레벨은 제어 노드에서 각 데이터 노드로 복제되어 일치합니다.

개별 노드가 아니라 전체 피처 클러스터에 라이선스를 할당합니다. 그러나 클러스터의 각 노드는 각 기능에 대한 별도 라이선스를 사용합니다. 클러스터링 기능 자체에는 라이선스가 필요하지 않습니다.

management center에 제어 노드를 추가하는 경우 클러스터에 사용하려는 기능 라이선스를 지정할 수 있습니다. 클러스터를 생성하기 전에는 데이터 노드에 할당된 라이선스가 중요하지 않습니다. 제어 노드의 라이선스 설정은 각 데이터 노드에 복제됩니다. **Devices(디바이스) > Device Management(디바이스 관리) > Cluster(클러스터) > License(라이선스)** 영역에서 클러스터 라이선스를 수정할 수 있습니다.



참고 management center이 라이선스 되기 전에 (평가 모드에서 실행 되기 전에) 클러스터를 추가하는 경우, management center를 라이선스하면 클러스터에 정책 변경을 구축할 때 트래픽 중단이 발생할 수 있습니다. 라이선스 모드를 변경하면 모든 데이터 유닛이 클러스터를 벗어났다가 다시 참가합니다.

Threat Defense 가상 클러스터링의 요구 사항 및 사전 요건

모델 요구 사항

- FTDv5, FTDv10, FTDv20, FTDv30, FTDv50, FTDv100
- VMware 또는 KVM
- 2x2 구성 구성에서 2개의 호스트에 있는 클러스터의 노드는 최대 4개입니다. 따라서 4개의 노드로 구성된 클러스터가 되도록 2개의 호스트 각각(2x2)에 최대 2개 threat defense virtual를 구축하는 것이 좋습니다.

사용자 역할

- 관리자
- 액세스 관리자
- 네트워크 관리자

하드웨어 및 소프트웨어 요건

클러스터의 모든 유닛은 다음과 같아야 합니다.

- 클러스터 제어 링크에 대해 점보 프레임 예약이 활성화되어 있어야 합니다. "DeploymentType": "Cluster"를 설정하여 threat defense virtual를 구축할 때 Day 0 구성에서 점보 프레임 예약을 활성화할 수 있습니다. 그렇지 않으면 클러스터가 구성되고 정상 상태가 된 후 점보 프레임을 활성화하려면 각 노드를 다시 시작해야 합니다.
- KVM의 경우 CPU 하드 파티셔닝(CPU 피닝)을 사용해야 합니다.
- 동일한 성능 계층이어야 합니다. 모든 노드에 대해 동일한 수의 CPU 및 메모리를 사용하는 것이 좋습니다. 그렇지 않으면 성능이 가장 낮은 노드와 일치하도록 모든 노드에서 제한됩니다.
- management center 액세스는 관리 인터페이스에서 이루어져야 합니다. 데이터 인터페이스 관리 는 지원되지 않습니다.
- 이미지 업그레이드 시간을 제외하고는 동일한 소프트웨어를 실행해야 합니다. 무중단 업그레이드가 지원됩니다.
- 동일한 도메인에 있어야 합니다.

- 동일한 그룹에 있어야 합니다.
- 보류 중이거나 진행 중인 구축이 없어야 합니다.
- 제어 노드에 지원되지 않는 기능이 구성되어서는 안 됩니다(지원되지 않는 기능 및 클러스터링, 36 페이지 참조).
- 데이터 노드에는 VPN이 구성되지 않아야 합니다. 제어 노드는 사이트 간 VPN을 구성할 수 있습니다.

Management Center 필수조건

- management center NTP 서버가 모든 클러스터 노드에서 연결할 수 있는 신뢰할 수 있는 서버로 설정되어 있는지 확인합니다. 기본적으로 threat defense virtual는 management center와 동일한 NTP 서버를 사용합니다. 시간이 모든 클러스터 노드에서 동일하게 설정되지 않은 경우 클러스터에서 제거할 수 있습니다.

스위치 요구 사항

- 클러스터링을 구성하기 전에 스위치 구성을 완료해야 합니다. 클러스터 제어 링크에 연결된 포트에 올바른(더 높은) MTU가 구성되어 있는지 확인합니다. 기본적으로 클러스터 제어 링크 MTU는 데이터 인터페이스보다 154바이트 높게 설정됩니다. 스위치에 MTU가 일치하지 않으면 클러스터 형성이 실패합니다.

Threat Defense 가상 클러스터링에 대한 지침

고가용성

고가용성은 클러스터링에서 지원되지 않습니다.

IPv6

클러스터 제어 링크는 IPv4를 사용하는 경우에만 지원됩니다.

추가 지침

- 중요한 토폴로지 변경 사항(예: EtherChannel 인터페이스 추가 또는 제거, threat defense 또는 스위치의 인터페이스 활성화 또는 비활성화, 추가 스위치를 추가하여 VSS 또는 vPC 구성)이 발생할 경우 상태 검사 기능을 비활성화하고 비활성화된 인터페이스에 대해 인터페이스 모니터링도 비활성화해야 합니다. 토폴로지 변경이 완료되고 구성 변경 사항이 모든 유닛과 동기화되면 인터페이스 상태 검사 기능을 다시 활성화할 수 있습니다.
- 기존 클러스터에 유닛을 추가하거나 유닛을 다시 로드할 경우, 일시적이고 제한적으로 패킷/연결이 감소하며 이는 정상적인 동작입니다. 경우에 따라 감소된 패킷으로 인해 연결이 끊어질 수 있습니다. 예를 들어, FTP 연결의 FIN/ACK 패킷이 감소할 경우 FTP 클라이언트가 끊어집니다. 이 경우 FTP 연결을 다시 설정해야 합니다.

- 암호 해독된 TLS/SSL 연결의 경우, 암호 해독 상태가 동기화되지 않습니다. 연결 소유자 장애가 발생하는 경우, 암호 해독된 연결이 재설정됩니다. 새 유닛에 새 연결을 설정해야 합니다. 암호 해독되지 않은 연결(암호 해독 안 함 규칙과 일치하는 연결)은 영향을 받지 않으며, 올바르게 복제됩니다.
- 데이터 인터페이스에는 VXLAN이 지원되지 않습니다. 클러스터 제어 링크만 VXLAN을 지원합니다.

클러스터링 기본값

- cLACP 시스템 ID가 자동 생성되며 시스템 우선순위는 기본적으로 1입니다.
- 클러스터 상태 검사 기능은 기본적으로 활성화되어 있으며 3초간의 대기 시간이 있습니다. 인터페이스 상태 모니터링은 모든 인터페이스에서 기본적으로 활성화됩니다.
- 장애가 발생한 클러스터 제어 링크에 대한 클러스터 자동 다시 참가 기능은 5분마다 무제한으로 시도됩니다.
- 장애가 발생한 데이터 인터페이스에 대한 클러스터 자동 다시 참가 기능은 간격이 2로 늘어 5분마다 3번 시도됩니다.
- 5초 연결 복제 지연은 HTTP 트래픽에 대해 기본적으로 활성화되어 있습니다.

Threat Defense 가상 클러스터링 구성

threat defense virtual 구축 후 클러스터링을 구성하려면 다음 작업을 수행합니다.

Management Center에 디바이스 추가

클러스터링을 구성하기 전에 각 클러스터 노드를 구축한 다음 management center에서 디바이스를 독립형 유닛으로 추가합니다.

프로시저

단계 1 [Cisco Secure Firewall Threat Defense Virtual 시작 가이드](#)에 따라 각 클러스터 노드를 구축합니다.

클러스터의 모든 유닛은 다음과 같아야 합니다.

- 클러스터 제어 링크에 대해 점보 프레임 예약이 활성화되어 있어야 합니다. "DeploymentType": "Cluster"를 설정하여 threat defense virtual를 구축할 때 Day 0 구성에서 점보 프레임 예약을 활성화할 수 있습니다. 그렇지 않으면 클러스터가 구성되고 정상 상태가 된 후 점보 프레임을 활성화하려면 각 노드를 다시 시작해야 합니다.
- KVM의 경우 CPU 하드 파티셔닝(CPU 피닝)을 사용해야 합니다.

단계 2 각 노드를 동일한 도메인 및 그룹에서 독립형 디바이스로 management center에 추가합니다.

Management Center에 디바이스 추가의 내용을 참조하십시오. 단일 디바이스로 클러스터를 생성한 다음 나중에 노드를 더 추가할 수 있습니다. 디바이스를 추가할 때 설정하는 초기 설정(라이선싱, 액세스 제어 정책)은 제어 노드의 모든 클러스터 노드에 상속됩니다. 클러스터를 구성할 때 제어 노드를 선택합니다.

클러스터 생성

management center에서 하나 이상의 디바이스에서 클러스터를 형성합니다.

시작하기 전에

일부 기능은 클러스터링과 호환되지 않으므로 클러스터링을 활성화할 때까지 기다려야 구성을 수행할 수 있습니다. 일부 기능은 이미 구성된 경우 클러스터 생성을 차단합니다. 예를 들어 인터페이스에서 IP 주소를 구성하거나 BVI와 같이 지원되지 않는 인터페이스 유형을 구성하지 마십시오.

프로시저

단계 1 Devices(디바이스) > Device Management(디바이스 관리)를 선택하고 Add(추가) > Add Cluster(클러스터 추가)를 선택합니다.

Add Cluster Wizard(클러스터 추가 마법사)가 나타납니다.

그림 1: 클러스터 추가 마법사

Add Cluster Wizard

1 Configuration — 2 Summary

▲ Create a cluster for supported models. Note: For the Firepower 4100/9300/AWS/Azure/GCP, use the Add Device option.

Cluster Name*
cluster1

Cluster Key
....
....

Control Node
You can form the cluster with just the control node to reduce formation time.
Node*
node1

VXLAN Network Identifier (VNI) Network* / 27 (30 addresses) Virtual Tunnel Endpoint (VTEP) Network* / 27 (30 addresses)
10.10.1.0 / 27 (30 addresses) 209.165.200.224 / 27 (30 addresses)

Cluster Control Link* VTEP IPv4 Address* Priority*
GigabitEthernet0/7 209.165.200.225 1

Data Nodes (Optional)
Data node hardware needs to match the control node hardware.
[Add a data node](#)

단계 2 제어 트래픽에 대한 클러스터 이름 및 인증 클러스터 키를 지정합니다.

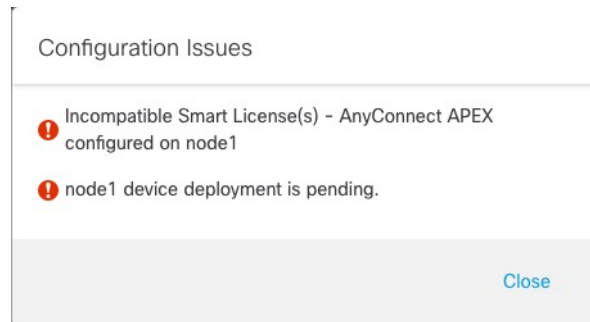
- **Cluster Name**(클러스터 이름)—1자 ~ 38자로 된 ASCII 문자열입니다.
- **Cluster Key**(클러스터 키)—1자 ~ 63자로 된 ASCII 문자열입니다. **Cluster Key**(클러스터 키)는 암호화 키를 생성하는 데 사용됩니다. 이 암호화는 연결 상태 업데이트 및 전달된 패킷을 비롯한 데이터 경로 트래픽에 영향을 미치지 않으며, 항상 일반 텍스트로 전송됩니다.

단계 3 제어 노드에 대해 다음을 설정합니다.

- **Node**(노드) — 초기에 제어 노드로 사용할 디바이스를 선택합니다. **management center**는 클러스터를 구성할 때 이 노드를 먼저 클러스터에 추가하므로 제어 노드가 됩니다.

참고 노드 이름 옆에 **Error**(오류) (❗) 아이콘이 표시되면 아이콘을 클릭하여 구성 문제를 확인합니다. 클러스터 형성을 취소하고 문제를 해결한 다음 클러스터 형성으로 돌아가야 합니다. 예를 들면 다음과 같습니다.

그림 2: 구성 문제



위의 문제를 해결하려면 지원되지 않는 VPN 라이선스를 제거하고 보류 중인 구성 변경 사항을 디바이스에 구축합니다.

- **VNI(VXLAN Network Identifier)** 네트워크 - VNI 네트워크에 대한 IPv4 서브넷을 지정합니다. 이 네트워크에는 IPv6가 지원되지 않습니다. **24, 25, 26** 또는 **27** 서브넷을 지정합니다. IP 주소가 이 네트워크의 각 노드에 자동으로 할당됩니다. VNI 네트워크는 물리적 VTEP 네트워크에서 실행되는 암호화된 가상 네트워크입니다.
- **Cluster Control Link**(클러스터 제어 링크) - 클러스터 제어 링크에 사용할 물리적 인터페이스를 선택합니다.
- **VTEP(Virtual Tunnel Endpoint)** 네트워크 - 물리적 인터페이스 네트워크에 대한 IPv4 서브넷을 지정합니다. 이 네트워크에는 IPv6가 지원되지 않습니다. VTEP 네트워크는 VNI 네트워크와 다른 네트워크이며 물리적 클러스터 제어 링크에 사용됩니다.
- **VTEP IPv4 Address(VTEP IPv4 주소)**—이 필드는 VTEP 네트워크의 첫 번째 주소로 자동 채워집니다.
- **Priority**(우선순위) — 제어 노드 선택을 위해 이 노드의 우선순위를 설정합니다. 우선순위는 1에서 100까지이며 1이 가장 높은 우선순위입니다. 우선순위를 다른 노드보다 낮게 설정한 경우에도 클러스터가 처음 구성될 때 이 노드는 여전히 제어 노드가 됩니다.

단계 4 **Data Nodes (Optional)**(데이터 노드(선택 사항))에서 **Add a data node**(데이터 노드 추가)를 클릭하여 클러스터에 노드를 추가합니다.

더 빠른 클러스터 형성을 위해 제어 노드만 사용하여 클러스터를 형성하거나 모든 노드를 지금 추가할 수 있습니다. 각 데이터 노드에 대해 다음을 설정합니다.

- **Node(노드)** — 추가할 디바이스를 선택합니다.

참고 노드 이름 옆에 **Error(오류)** (❗) 아이콘이 표시되면 아이콘을 클릭하여 구성 문제를 확인합니다. 클러스터 형성을 취소하고 문제를 해결한 다음 클러스터 형성으로 돌아가야 합니다.

- **VTEP IPv4 Address(VTEP IPv4 주소)**—이 필드는 VTEP 네트워크의 다음 주소로 자동 채워집니다.
- **Priority(우선순위)** — 제어 노드 선택을 위해 이 노드의 우선순위를 설정합니다. 우선순위는 1에서 100까지이며 1이 가장 높은 우선순위입니다.

단계 5 **Continue**(계속)를 클릭합니다. **Summary**(요약)를 검토하고 **Save**(저장)를 클릭합니다.

클러스터 부트스트랩 구성이 클러스터 노드에 저장됩니다. 부트스트랩 구성에는 클러스터 제어 링크에 사용되는 VXLAN 인터페이스가 포함됩니다.

디바이스 > 디바이스 관리 페이지에 클러스터 이름이 표시됩니다. 클러스터 노드를 보려면 클러스터를 확장합니다.

그림 3: 클러스터 관리

ftdcluster (2) Cluster						
172.16.0.50 (Control) 172.16.0.50 - Routed	Snort 3	FTDv for VMware	7.2.0	Manage	Base, Threat (2 more...)	Default AC Policy
172.16.0.51 172.16.0.51 - Routed	Snort 3	FTDv for VMware	7.2.0	N/A	Base, Threat (2 more...)	Default AC Policy

현재 등록되는 노드에는 로딩 아이콘이 표시됩니다.

그림 4: 노드 등록

ftdcluster (2) Cluster	
172.16.0.50 (Control) 172.16.0.50 - Routed	Snort 3
172.16.0.51 172.16.0.51 - Routed	Snort 3

알림 아이콘을 클릭하고 작업을 선택하여 클러스터 노드 등록을 모니터링할 수 있습니다. **management center**은 각 노드가 등록될 때마다 클러스터 등록 작업을 업데이트합니다.

Deployment ID	Status	Message	Completion Time
10.10.1.12	Success	Deployment to device successful.	1m 54s
10.10.1.13	Success	Deployment to device successful.	1m 3s
TD_Cluster	Success	Deployment to device successful.	35s

단계 6 클러스터에 대해 **Edit(수정)** (✎)을 클릭하여 디바이스별 설정을 구성합니다.

대부분의 구성은 클러스터의 노드가 아닌 클러스터 전체에 적용할 수 있습니다. 예를 들어 노드당 표시 이름을 변경할 수 있지만 전체 클러스터에 대해서만 인터페이스를 설정할 수 있습니다.


단계 7 **Devices(디바이스) > Device Management(디바이스 관리) > Cluster(클러스터)** 화면에서 **General(일반)** 및 클러스터에 대한 기타 설정을 표시합니다.

그림 5: 클러스터 설정

Section	Parameter	Value
General	Name	ftdcluster
	Transfer Packets	No
	Status	●
	Control	172.16.0.50
	Cluster Live Status	View
License	Base	Yes
	Export-Controlled Features	No
	Malware	Yes
	Threat	Yes
	URL Filtering	Yes
	AnyConnect Apex	N/A
Security Engine	Intrusion Prevention Engine	Snort 3.0
Applied Policies	Access Control Policy	Default AC Policy
	Prefilter Policy	Default Prefilter Policy
	SSL Policy	
	DNS Policy	Default DNS Policy
	Identity Policy	
	NAT Policy	
	Platform Settings Policy	
	NGFW QoS Policy	
	FlexConfig Policy	
	Advanced Settings	Application Bypass
Bypass Threshold		3000 ms
Interface Object Optimization		Disabled

General(일반) 영역에서 다음 클러스터별 항목을 참조하십시오.


- **General (일반) > Name (이름) - Edit(수정)** (✎)를 클릭하여 클러스터 표시 이름을 변경합니다.

General	
Name:	ftdcluster
Transfer Packets:	No
Status:	
Control:	172.16.0.50
Cluster Live Status:	View

그런 다음 **Name**(이름) 필드를 설정합니다.

General	
Name:	<input type="text" value="ftdcluster"/>
Transfer Packets:	<input type="checkbox"/>
Compliance Mode:	
TLS Crypto Acceleration:	
Force Deploy:	→

- **General**(일반) > **View**(보기)—**View**(보기) 링크를 클릭하여 **Cluster Status**(클러스터 상태) 대화 상자를 엽니다.

General	
Name:	ftdcluster
Transfer Packets:	No
Status:	
Control:	172.16.0.50
Cluster Live Status:	View

Cluster Status(클러스터 상태) 대화 상자에서 **Reconcile All**(모두 조정)을 클릭하면 데이터 유닛 등록을 다시 시도할 수도 있습니다.

Cluster Status

Overall Status: Cluster has all nodes in sync

Nodes details (2) Refresh Reconcile All

	Status	Device Name	Unit Name	Chassis URL	
>	In Sync.	172.16.0.50 Control	172.16.0.50	N/A	⋮
>	In Sync.	172.16.0.51	172.16.0.51	N/A	⋮


Dated: 11:52:26 | 20 Dec 2021 Close

단계 8 **Devices**(디바이스) > **Device Management**(디바이스 관리) > 디바이스(디바이스)의 오른쪽 상단 드롭 다운 메뉴에서 클러스터의 각 멤버를 선택하고 다음 설정을 구성할 수 있습니다.

그림 6: 디바이스 설정

그림 7: 노드 선택

- **General**(일반) > **Name** (이름) - **Edit**(수정) (✎)을 클릭하여 클러스터 멤버 표시 이름을 변경합니다.

General 	
Name:	10.89.5.21
Transfer Packets:	Yes
Mode:	routed
Compliance Mode:	None
TLS Crypto Acceleration:	Enabled

그런 다음 **Name**(이름) 필드를 설정합니다.

General ?

Name:

Transfer Packets:

Mode: routed


Compliance Mode: None

Performance Profile: Default

TLS Crypto Acceleration: Disabled

Force Deploy: →

- **Management(관리) > Host(호스트)**—디바이스 구성에서 관리 IP 주소를 변경하는 경우 새 주소를 management center에 일치시켜야 네트워크의 디바이스와 연결할 수 있습니다. 먼저 연결을 비활성화하고 **Management(관리)** 영역에서 **Host(호스트)** 주소를 편집한 다음 연결을 다시 활성화합니다.

Management 	
Host:	10.89.5.20
Status:	✓

단계 9 점보 프레임 예약을 활성화하지 않고 클러스터 노드를 구축한 경우 모든 클러스터 노드를 다시 시작하여 클러스터 제어 링크에 필요한 점보 프레임을 활성화합니다. **디바이스 종료 또는 재시작**을 참조하십시오.

이전에 점보 프레임 예약을 활성화한 경우 이 단계를 건너뛸 수 있습니다.

클러스터 제어 링크 트래픽에는 데이터 패킷 전달이 포함되므로 클러스터 제어 링크는 데이터 패킷의 전체 크기와 클러스터 트래픽 오버헤드(100바이트) 및 VXLAN 오버헤드(54바이트)를 모두 수용해야 합니다. 클러스터를 생성할 때 MTU는 최고 데이터 인터페이스 MTU(기본값: 1654)보다 154바

이트 더 높게 설정됩니다. 나중에 데이터 인터페이스 MTU를 늘리면 클러스터 제어 링크 MTU도 늘립니다. 예를 들어 최대 MTU가 9198바이트이므로 가장 높은 데이터 인터페이스 MTU는 9044가 될 수 있는 반면, 클러스터 제어 링크는 9198로 설정할 수 있습니다. [MTU 구성](#) 섹션을 참조하십시오.

참고 클러스터 제어 링크에 연결된 스위치를 올바른 (상위) MTU로 구성해야 합니다. 그렇지 않으면 클러스터 형성이 실패합니다.

인터페이스 구성

이 섹션에서는 클러스터링과 호환되는 개별 인터페이스를 구성하는 방법에 대해 설명합니다. 개별 인터페이스는 정상적인 라우팅 인터페이스로, 각각 IP 주소 풀에서 가져온 고유한 IP 주소가 있습니다. 기본 클러스터 IP 주소는 현재 제어 노드에 항상 속해 있는 클러스터의 고정 주소입니다. 모든 데이터 인터페이스는 개별 인터페이스여야 합니다.

진단 인터페이스의 경우 IP 주소 풀을 구성하거나 DHCP를 사용할 수 있습니다. 진단 인터페이스만 DHCP에서 주소 가져오기를 지원합니다. DHCP를 사용하려면 이 절차를 사용하지 마십시오. 대신 주소와 같이 구성합니다([라우팅 모드 인터페이스 구성](#) 참조).



참고 하위 인터페이스를 사용할 수 없습니다.

프로시저

- 단계 1 IPv4 및/또는 IPv6 주소 풀을 추가하려면 **Objects(개체) > Object Management(개체 관리) > Address Pools(주소 풀)**을 선택합니다. [주소 풀](#)을 참조하십시오.

최소한 클러스터에 있는 유닛 수에 상응하는 개수의 주소를 포함해야 합니다. 가상 IP 주소가 이 풀의 일부가 아니어도 동일한 네트워크에 있어야 합니다. 사전에 각 장치에 할당된 정확한 로컬 주소를 확인할 수 없습니다.
- 단계 2 디바이스 > 디바이스 관리를 선택하고 클러스터 옆의 **Edit(수정)** (✎)를 클릭합니다.
- 단계 3 **Interfaces(인터페이스)**를 클릭한 다음 데이터 인터페이스에 대해 **Edit(수정)** (✎)을 클릭합니다.
- 단계 4 **IPv4**에서 **IP** 주소 및 마스크를 입력합니다. IP 주소는 현재 제어 유닛에 항상 속해 있는 클러스터의 고정 주소입니다.
- 단계 5 **IPv4 Address Pool(IPv4 주소 풀)** 드롭다운 목록에서 생성한 주소 풀을 선택합니다.

참고 이 인터페이스에 MAC 주소를 수동으로 할당하려면 FlexConfig를 사용하여 **mac-address pool**를 생성해야 합니다.
- 단계 6 **IPv6 > Basic(기본)**의 **IPv6 Address Pool(IPv6 주소 풀)** 드롭다운 목록에서 생성한 주소 풀을 선택합니다.
- 단계 7 다른 인터페이스 설정은 기본으로 구성합니다.

단계 8 **Save**(저장)를 클릭합니다.

이제 **Deploy**(구축) > **Deployment**(구축)로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

클러스터 상태 모니터링 설정 구성

Cluster(클러스터) 페이지의 **Cluster Health Monitor Settings**(클러스터 상태 모니터링 설정) 섹션은 아래 표의 설정을 표시합니다.

그림 8: 클러스터 상태 모니터링 설정

Cluster Health Monitor Settings			
Timeouts			
Hold Time			3 s
Interface Debounce Time			9000 ms
Monitored Interfaces			
Service Application			Enabled
Unmonitored Interfaces			None
Auto-Rejoin Settings			
	Attempts	Interval Between Attempts	Interval Variation
Cluster Interface	-1	5	1
Data Interface	3	5	2
System	3	5	2

표 1: 클러스터 상태 모니터링 설정 섹션 표 필드

필드	설명
시간 초과	
보류 시간	노드 시스템 상태를 확인하기 위해 클러스터 노드에서는 다른 노드에 대한 클러스터 제어 링크에서 하트비트 메시지를 보냅니다. 노드가 피어 노드의 하트비트 메시지를 대기 시간 내에 수신하지 않을 경우, 해당 피어 노드는 응답하지 않거나 중지된 상태로 간주됩니다.
인터페이스 디바운스 시간	인터페이스 디바운스 시간은 노드가 인터페이스에 장애가 발생한 것으로 간주하고 노드가 클러스터에서 제거되기 전까지의 시간입니다.

필드	설명
모니터링 인터페이스	인터페이스 상태 검사에서는 링크 오류 여부를 모니터링합니다. 지정된 논리적 인터페이스에 대한 모든 물리적 포트가 특정 노드에서 오류가 발생했지만 다른 노드에 있는 동일한 논리적 인터페이스에서 활성 포트가 있는 경우 이 노드는 클러스터에서 제거됩니다. 노드에서 클러스터의 멤버를 제거하기 전까지 걸리는 시간은 인터페이스의 유형에 따라, 그리고 해당 노드가 설정된 노드인지 또는 클러스터에 참가하는지에 따라 달라집니다.
서비스 애플리케이션	Snort 및 disk-full 프로세스의 모니터링 여부를 표시합니다.
모니터링되지 않는 인터페이스	모니터링되지 않는 인터페이스를 표시합니다.
자동 재연결 설정	
클러스터 인터페이스	클러스터 제어 링크 장애에 대한 자동 다시 참가 설정을 표시합니다.
데이터 인터페이스	데이터 인터페이스 실패에 대한 자동 다시 참가 설정을 표시합니다.
시스템	내부 오류에 대한 자동 다시 참가 설정을 표시합니다. 내부 오류 포함: 애플리케이션 동기화 시간 초과, 일치하지 않는 애플리케이션 상태 등



참고 시스템 상태 확인을 비활성화하면 시스템 상태 확인이 비활성화되었을 때 적용되지 않는 필드가 표시되지 않습니다.

이 섹션에서 이러한 설정을 할 수 있습니다.

모든 포트 채널 ID, 단일 물리적 인터페이스 ID는 물론 Snort 및 디스크 전체 프로세스도 모니터링할 수 있습니다. 상태 모니터링은 VNI 또는 BVI 같은 VLAN 하위 인터페이스 또는 가상 인터페이스에서 수행되지 않습니다. 클러스터 제어 링크의 모니터링을 구성할 수 없습니다. 이 링크는 항상 모니터링됩니다.


프로시저

단계 1 **Devices(디바이스) > Device Management(디바이스 관리)**을(를) 선택합니다.

단계 2 수정할 클러스터 옆의 **Edit(수정)**()을 클릭합니다.

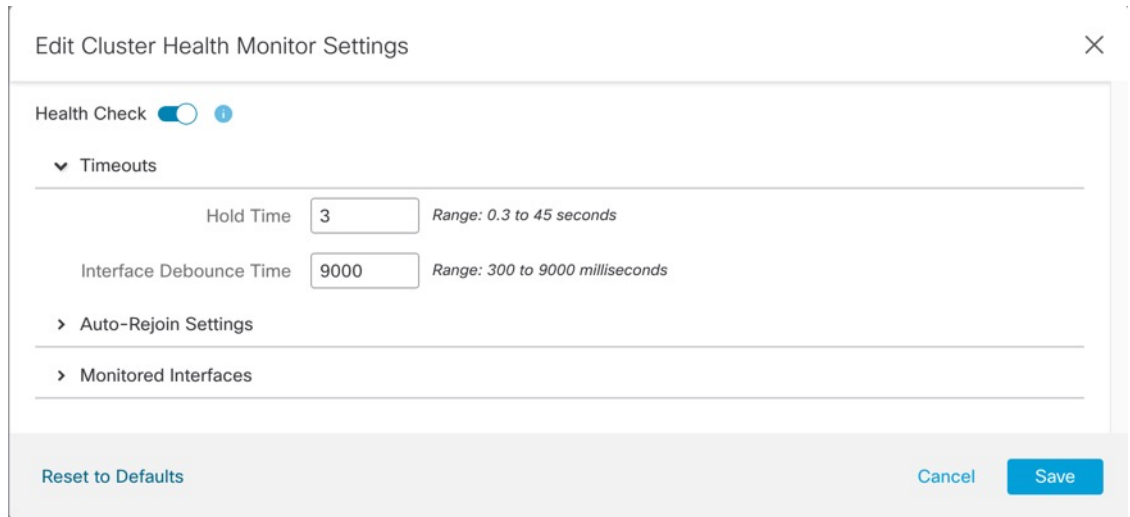
다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 3 **Cluster(클러스터)**를 클릭합니다.

단계 4 **Cluster Health Monitor Settings(클러스터 상태 모니터링 설정)** 섹션에서 **Edit(수정)**()을 클릭합니다.

단계 5 Health Check(상태 확인) 슬라이더를 클릭하여 시스템 상태 확인을 비활성화합니다.

그림 9: 시스템 상태 확인 비활성화



토폴로지 변경 사항(예: 데이터 인터페이스 추가 또는 제거, 노드 또는 스위치의 인터페이스 활성화 또는 비활성화, 추가 스위치를 추가하여 VSS 또는 vPC 구성)이 발생할 경우 시스템 상태 검사 기능을 비활성화하고 비활성화된 인터페이스에 대한 인터페이스 모니터링도 비활성화해야 합니다. 토폴로지 변경이 완료되고 구성 변경 사항이 모든 노드와 동기화되면 시스템 상태 검사 기능 및 모니터링되는 인터페이스를 다시 활성화할 수 있습니다.

단계 6 보류 시간 및 인터페이스 디바운스 시간을 구성합니다.

- 보류 시간—노드 하트비트 상태 메시지 사이의 시간을 결정하는 보류 시간을 0.3초에서 45초 사이로 설정합니다. 기본값은 3초입니다.
- **Interface Debounce Time**(인터페이스 디바운스 시간)—디바운스 시간을 300~9000밀리초 범위에서 설정합니다. 기본값은 500ms입니다. 값이 낮을수록 인터페이스 오류 탐지를 더 빠르게 수행할 수 있습니다. 디바운스 시간을 더 낮게 구성하면 오탐의 가능성이 증가합니다. 인터페이스 상태 업데이트가 발생하는 경우, 인터페이스를 실패로 표시하고 노드가 클러스터에서 제거되기 전에 노드는 지정되어 있는 밀리초 동안 대기합니다. 가동 중단 상태에서 가동 상태로 전환되는 EtherChannel의 경우(예: 스위치 다시 로드됨 또는 EtherChannel에서 스위치 활성화됨), 디바운스 시간이 더 길어 다른 클러스터 노드가 포트 번들링 시 더 빨랐다는 이유만으로 인터페이스가 클러스터 노드에서 실패한 것으로 표시되는 것을 방지할 수 있습니다.

단계 7 상태 검사에 실패한 후에 자동 다시 참가 클러스터 설정을 맞춤화합니다.

그림 10: 자동 재연결 설정 구성

▼ Auto-Rejoin Settings

Cluster Interface

Attempts Range: 0-65535 (-1 for unlimited number of attempts)

Interval Between Attempts Range: 2-60 minutes between rejoin attempts

Interval Variation Range: 1-3. Defines if the interval duration increases. 1 (no change); 2 (2 x the previous duration), or 3 (3 x the previous duration).

Data Interface

Attempts Range: 0-65535 (-1 for unlimited number of attempts)

Interval Between Attempts Range: 2-60 minutes between rejoin attempts

Interval Variation Range: 1-3. Defines if the interval duration increases. 1 (no change); 2 (2 x the previous duration), or 3 (3 x the previous duration).

System

Attempts Range: 0-65535 (-1 for unlimited number of attempts)

Interval Between Attempts Range: 2-60 minutes between rejoin attempts

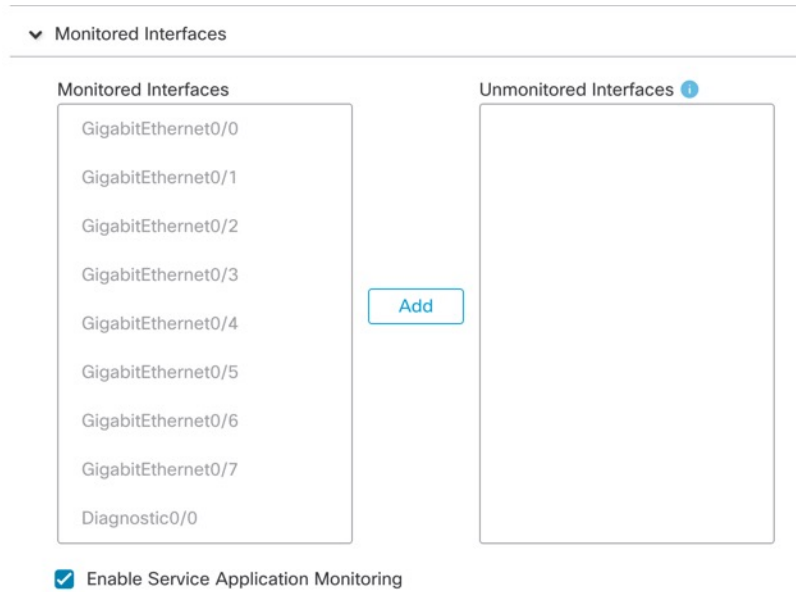
Interval Variation Range: 1-3. Defines if the interval duration increases. 1 (no change); 2 (2 x the previous duration), or 3 (3 x the previous duration).

Cluster Interface(클러스터 인터페이스), **Data Interface**(데이터 인터페이스) 및 **System**(시스템)에 대해 다음 값을 설정합니다(내부 장애에는 애플리케이션 동기화 시간 초과, 일관되지 않은 애플리케이션 상태 등이 포함됨).

- **Attempts**(시도 횟수) — 다시 참가 시도 횟수를 -1~65535 범위에서 설정합니다. **0**은 자동 다시 참가를 비활성화합니다. **Cluster Interface**(클러스터 인터페이스)의 기본값은 -1(무제한)입니다. **Data Interface**(데이터 인터페이스) 및 **System**(시스템)의 기본값은 3입니다.
- **Interval Between Attempts**(시도 간의 간격) — 다시 참가 시도 간의 간격 기간(분)을 2~60분 사이로 정의합니다. 기본값은 5분입니다. 노드가 클러스터에 다시 조인하려고 시도하는 최대 총 시간은 마지막 장애 시간으로부터 14400분(10일)으로 제한됩니다.
- **Interval Variation**(간격 변동) — 간격 기간이 증가하는지 여부를 정의합니다. 1~3 사이의 값 설정: **1**(변경 없음), **2**(2 x 이전 기간) 또는 **3**(3 x 이전 기간)입니다. 예를 들어, 간격 기간을 5분으로 설정하고 변수를 2로 설정하면 첫 번째 시도가 5분 후에 일어나고 두 번째 시도는 10분(2 x 5), 세 번째 시도는 20분(2 x 10) 후에 일어납니다. 기본값은 **Cluster Interface**(클러스터 인터페이스)의 경우 **1**이고 **Data Interface**(데이터 인터페이스) 및 **System**(시스템)의 경우 **2**입니다.

단계 8 **Monitored Interfaces**(모니터링된 인터페이스) 또는 **Unmonitored Interfaces**(모니터링되지 않는 인터페이스) 창에서 인터페이스를 이동하여 모니터링되는 인터페이스를 구성합니다. 또한 **Enable Service Application Monitoring**(서비스 애플리케이션 모니터링 활성화)을 선택하거나 선택 취소하여 Snort 및 디스크 팩 찬 프로세스의 모니터링을 활성화하거나 비활성화할 수 있습니다.

그림 11: 모니터링되는 인터페이스 구성



인터페이스 상태 검사에서는 링크 오류 여부를 모니터링합니다. 지정된 논리적 인터페이스에 대한 모든 물리적 포트가 특정 노드에서 오류가 발생했지만 다른 노드에 있는 동일한 논리적 인터페이스에서 활성 포트가 있는 경우 이 노드는 클러스터에서 제거됩니다. 노드에서 클러스터의 멤버를 제거하기 전까지 걸리는 시간은 인터페이스의 유형에 따라, 그리고 해당 노드가 설정된 노드인지 또는 클러스터에 참가하는지에 따라 달라집니다. 상태 검사는 모든 인터페이스와 Snort 및 디스크 풀 프로세스에 대해 기본적으로 활성화됩니다.

필수가 아닌 인터페이스(예: 진단 인터페이스)에 대한 상태 모니터링을 비활성화할 수 있습니다.

토폴로지 변경 사항(예: 데이터 인터페이스 추가 또는 제거, 노드 또는 스위치의 인터페이스 활성화 또는 비활성화, 추가 스위치를 추가하여 VSS 또는 vPC 구성)이 발생할 경우 시스템 상태 검사 기능을 비활성화하고 비활성화된 인터페이스에 대한 인터페이스 모니터링도 비활성화해야 합니다. 토폴로지 변경이 완료되고 구성 변경 사항이 모든 노드와 동기화되면 시스템 상태 검사 기능 및 모니터링되는 인터페이스를 다시 활성화할 수 있습니다.

단계 9 **Save**(저장)를 클릭합니다.

단계 10 구성 변경 사항을 구축합니다. [구성 변경 사항 구축](#)의 내용을 참고하십시오.

클러스터 노드 관리

.

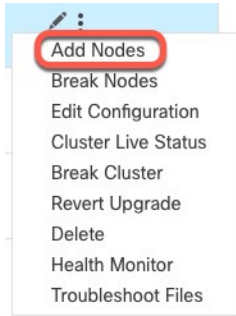
새 클러스터 노드 추가

기존 클러스터에 하나 이상의 새 클러스터 노드를 추가할 수 있습니다.

프로시저

단계 1 **Devices**(디바이스) > **Device Management**(디바이스 관리)를 선택하고 클러스터에 대해 추가 (+)를 클릭하고 **Add Nodes**(노드 추가)를 선택합니다.

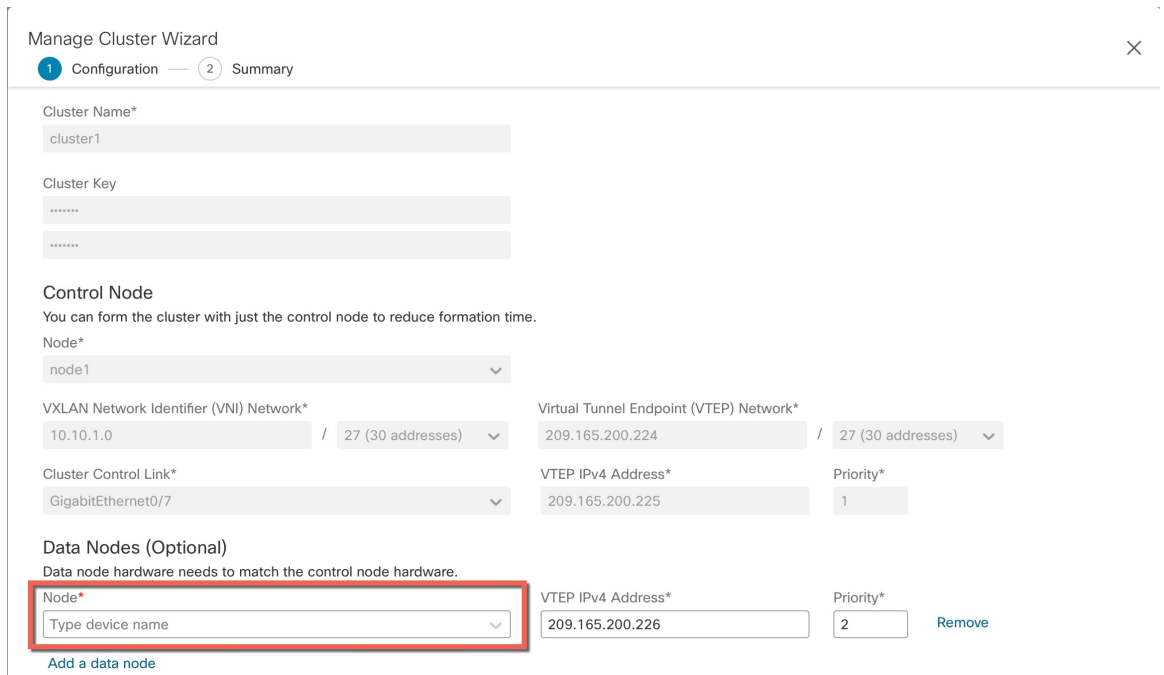
그림 12: 노드 추가



Manage Cluster Wizard(클러스터 관리 마법사)가 나타납니다.

단계 2 **Node**(노드) 메뉴에서 디바이스를 선택하고 원하는 경우 IP 주소 및 우선순위를 조정합니다.

그림 13: 클러스터 마법사 관리

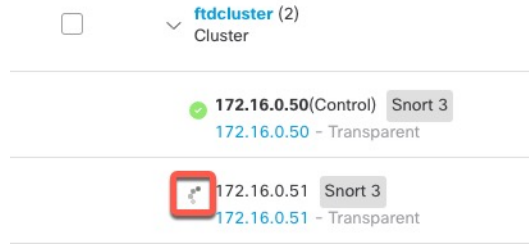


단계 3 노드를 추가하려면 **Add data node**(데이터 노드 추가)를 클릭합니다.

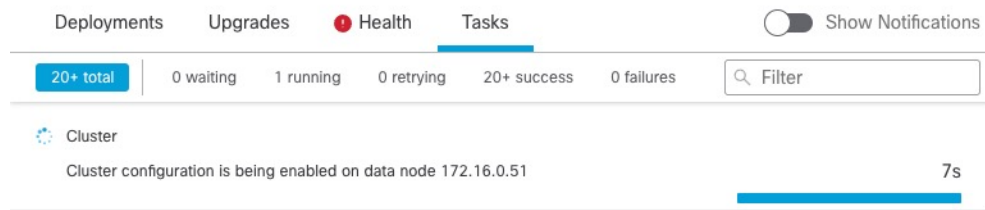
단계 4 **Continue**(계속)를 클릭합니다. **Summary**(요약)를 검토하고 **Save**(저장)를 클릭합니다.

현재 등록되는 노드에는 로딩 아이콘이 표시됩니다.

그림 14: 노드 등록



알림 아이콘을 클릭하고 작업을 선택하여 클러스터 노드 등록을 모니터링할 수 있습니다.



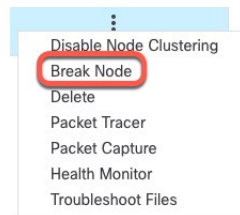
노드 분리

클러스터에서 노드를 제거하여 독립형 디바이스가 되도록 할 수 있습니다. 전체 클러스터를 분리하지 않는 한 제어 노드를 분리할 수 없습니다. 데이터 노드의 구성이 지워졌습니다.

프로시저

단계 1 **Devices**(디바이스) > **Device Management**(디바이스 관리)를 선택하고 분리할 노드의 추가 (⋮)을 클릭한 다음 **Break Node**(노드 분리)를 선택합니다.

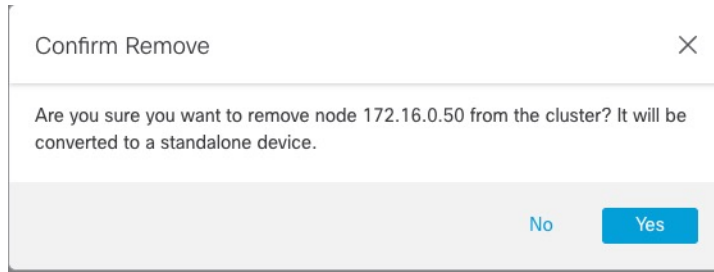
그림 15: 노드 분리



Break Nodes(노드 분리)를 선택하여 클러스터 **More**(추가) 메뉴에서 하나 이상의 노드를 분리할 수 있습니다.

단계 2 중단을 확인하라는 메시지가 표시됩니다. **Yes**(예)를 클릭합니다.

그림 16: 분리 확인



알림 아이콘을 클릭하고 작업을 선택하여 클러스터 노드 분리를 모니터링할 수 있습니다.

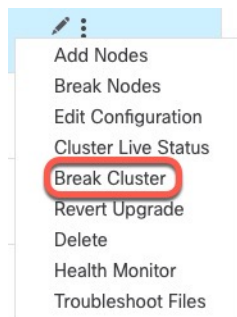
클러스터 분리

클러스터를 분리하고 모든 노드를 독립형 디바이스로 변환할 수 있습니다. 제어 노드는 인터페이스 및 보안 정책 구성을 유지하는 반면, 데이터 노드는 해당 구성을 지웁니다.

프로시저

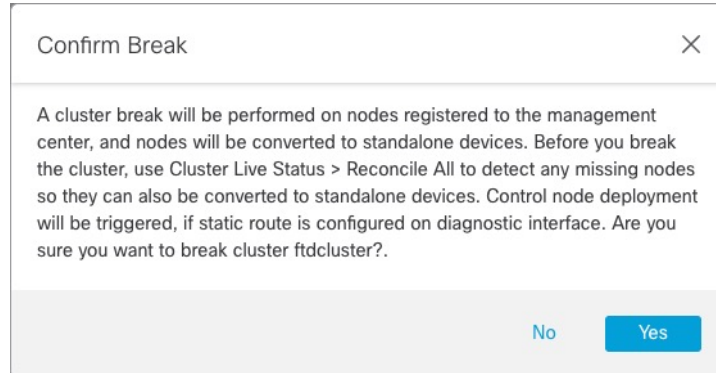
- 단계 1 노드를 조정하여 모든 클러스터 노드가 management center에서 관리되고 있는지 확인합니다. [클러스터 노드 조정, 28 페이지](#)의 내용을 참조하십시오.
- 단계 2 **Devices**(디바이스) > **Device Management**(디바이스 관리)를 선택하고 클러스터에 대해 추가 (+)를 클릭하고 **Break Cluster**(클러스터 분리)를 선택합니다.

그림 17: 클러스터 분리



- 단계 3 클러스터를 분리하라는 프롬프트가 표시됩니다. **Yes**(예)를 클릭합니다.

그림 18: 분리 확인



알림 아이콘을 클릭하고 작업을 선택하여 클러스터 분리를 모니터링할 수 있습니다.

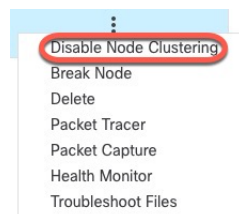
클러스터링 비활성화

노드 삭제를 준비하거나 유지 보수를 위해 일시적으로 노드를 비활성화할 수 있습니다. 이 절차는 노드를 일시적으로 비활성화하기 위함이며, **management center** 디바이스 목록에 노드를 유지해야 합니다. 노드가 비활성 상태가 되면 모든 데이터 인터페이스가 종료됩니다.

프로시저

- 단계 1** 비활성화하려는 유닛에 대해 **Devices(디바이스) > Device Management(디바이스 관리)**를 선택하고 추가 (⋮)를 클릭하고 **Disable Clustering(클러스터링 비활성화)**를 선택합니다.

그림 19: 클러스터링 비활성화



제어 노드에서 클러스터링을 비활성화하면 데이터 노드 중 하나가 새 제어 노드가 됩니다. 중앙 집중식 기능의 경우 제어 노드를 강제로 변경하면 모든 연결이 취소되며 새 제어 노드에서 연결을 다시 설정해야 합니다. 클러스터의 유일한 노드인 경우 제어 노드에서 클러스터링을 비활성화할 수 없습니다.

- 단계 2** 노드에서 클러스터링을 비활성화하고자 함을 확인합니다.

노드가 **Devices(디바이스) > Device Management(디바이스 관리)** 목록에서 그 이름 옆에 **(Disabled(비활성화 됨))**로 표시됩니다.

단계 3 클러스터링을 다시 활성화하려면 [클러스터 재참가, 26 페이지](#)의 내용을 참조하십시오.

클러스터 재참가

예를 들어 인터페이스 오류 등으로 노드가 클러스터에서 제거되거나 수동으로 클러스터링을 비활성화한 경우 클러스터를 수동으로 다시 참가시킬 수 있습니다. 클러스터 다시 조인을 시도하기 전에 오류가 해결되었는지 확인하십시오. 노드가 클러스터에서 제거되는 이유에 대한 자세한 내용은 [클러스터 다시 참가, 43 페이지](#)의 내용을 참조하십시오.

프로시저

단계 1 다시 활성화하려는 유닛에 대해 **Devices(디바이스) > Device Management(디바이스 관리)** 를 선택하고 추가 (+)를 클릭하고 **Enable Clustering(클러스터링 다시 활성화)**을 선택합니다.

단계 2 노드에서 클러스터링을 활성화하고자 함을 확인합니다.

제어 노드 변경



주의 제어 노드를 변경하는 가장 좋은 방법은 제어 노드의 클러스터링을 비활성화한 후 새 제어가 선택될 때까지 기다렸다가 클러스터링을 다시 활성화하는 것입니다. 제어 노드가 될 정확한 유닛을 지정해야 할 경우, 이 섹션의 절차를 참조하십시오. 중앙 집중식 기능의 경우 두 가지 방법을 사용하여 제어 노드를 강제로 변경하면 모든 연결이 취소되며 새 제어 노드에서 연결을 다시 설정해야 합니다.

제어 노드를 변경하려면 다음 단계를 수행합니다.

프로시저

단계 1 **Devices(디바이스) > Device Management(디바이스 관리) > 추가 (+) > Cluster Live Status(클러스터 라이브 상태)**를 선택하여 **Cluster Status(클러스터 상태)** 대화 상자를 엽니다.

그림 20: 클러스터 상태

Cluster Status ?

Overall Status: ✔ Cluster has all nodes in sync

Nodes details (2)

	Status	Device Name	Unit Name	Chassis URL	
>	In Sync.	172.16.0.50 Control	172.16.0.50	N/A	⋮
>	In Sync.	172.16.0.51	172.16.0.51	N/A	⋮

Dated: 11:52:26 | 20 Dec 2021

단계 2 제어 유닛이 될 유닛에 대해 추가 (⋮) **Change Role to Control**(역할을 제어로 변경)을 선택합니다.

단계 3 역할 변경을 확인하라는 메시지가 표시됩니다. 확인란을 선택하고 **OK**(확인)를 클릭합니다.

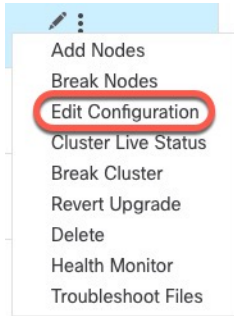
클러스터 구성 편집

클러스터 구성을 편집할 수 있습니다. 노드 또는 노드 우선순위에 대해 VTEP IP 주소 이외의 값을 변경하면 클러스터가 자동으로 중단되고 다시 구성됩니다. 클러스터를 재구성할 때까지 트래픽 중단이 발생할 수 있습니다. 노드 또는 노드 우선 순위의 VTEP IP 주소를 변경하면 영향을 받는 노드만 손상되어 클러스터에 다시 추가됩니다.

프로시저

단계 1 **Devices**(디바이스) > **Device Management**(디바이스 관리)를 선택하고 클러스터에 대해 추가 (⋮)를 클릭하고 **Edit Configuration**(구성 편집)을 선택합니다.

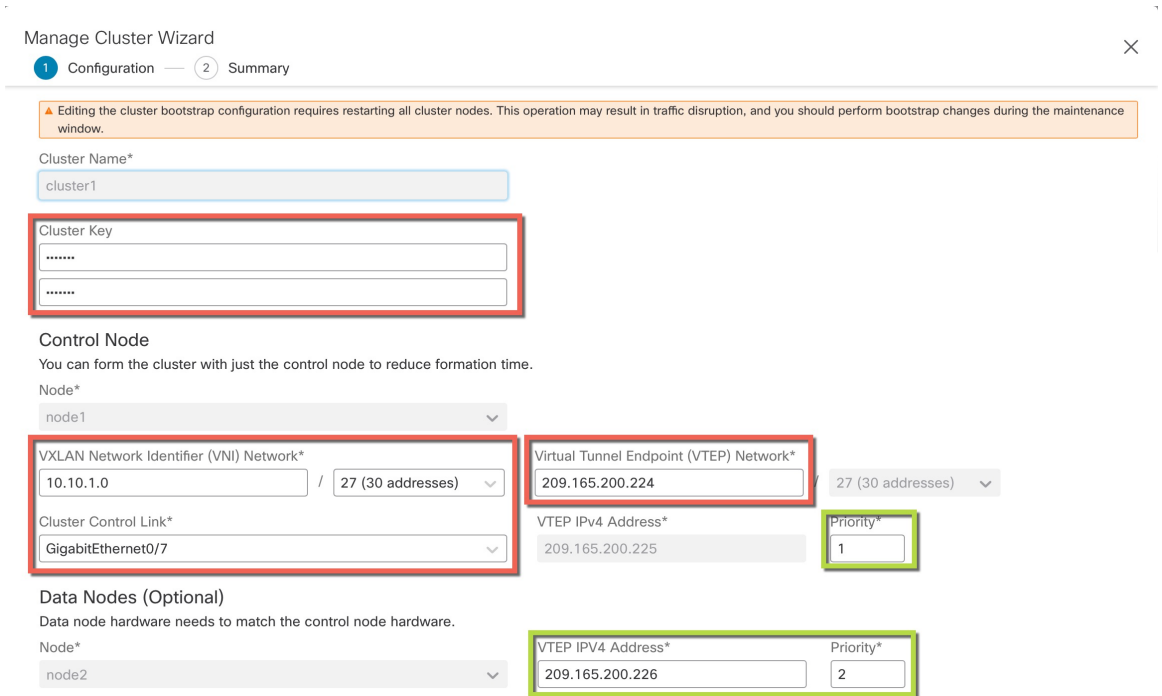
그림 21: 구성 편집



Manage Cluster Wizard(클러스터 관리 마법사)가 나타납니다.

단계 2 클러스터 구성을 업데이트합니다.

그림 22: 클러스터 마법사 관리



단계 3 **Continue**(계속)를 클릭합니다. **Summary**(요약)를 검토하고 **Save**(저장)를 클릭합니다.

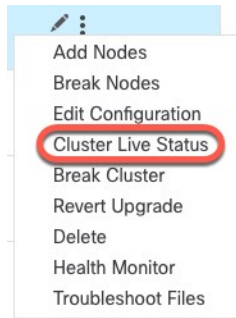
클러스터 노드 조정

클러스터 노드 등록에 실패하면 디바이스에서 **management center**에 대해 클러스터 멤버십을 다시 조정합니다. 예를 들어, **management center**이 특정 프로세스 중이거나 네트워크에 문제가 있는 경우, 데이터 노드 등록에 실패할 수 있습니다.

프로시저

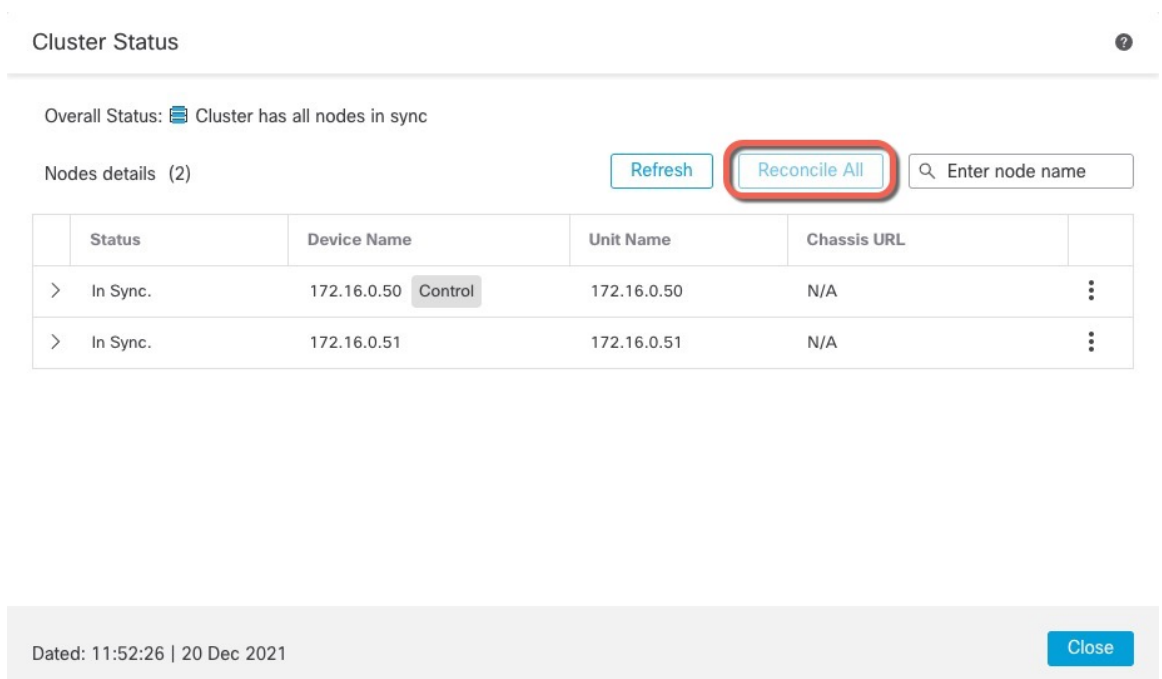
단계 1 클러스터에 대해 **Devices**(디바이스) > **Device Management**(디바이스 관리) 추가 (⋮)를 선택한 다음 **Cluster Live Status**(클러스터 라이브 상태)를 선택하여 **Cluster Status**(클러스터 상태) 대화 상자를 엽니다.

그림 23: 클러스터 라이브 상태



단계 2 **Reconcile All**(모두 조정)을 클릭합니다.

그림 24: 모두 조정



클러스터 상태에 대한 자세한 내용은 [클러스터 모니터링, 31 페이지](#)를 참고하십시오.

클러스터 또는 노드를 삭제(등록 해제)하고 새 Management Center에 등록

management center에서 클러스터를 등록 해제할 수 있습니다. 그래도 클러스터는 그대로 유지됩니다. 클러스터를 새 management center에 추가하려는 경우 클러스터를 등록 해제할 수 있습니다.

클러스터에서 노드를 분리하지 않고 management center에서 노드를 등록 해제할 수도 있습니다. 노드는 management center에 표시되지 않지만 여전히 클러스터의 일부이며 트래픽을 계속 전달하며 제어 노드가 될 수도 있습니다. 현재 제어 노드는 등록 해제할 수 없습니다. management center에서 더 이상 연결할 수 없지만 관리 연결 문제를 해결하는 동안 클러스터의 일부로 계속 유지하려는 경우 노드를 등록 해제할 수 있습니다.

클러스터 등록 해제:

- management center와 클러스터 간 모든 통신이 단절됩니다.
 - **Device Management**(디바이스 관리) 페이지에서 클러스터를 제거합니다.
 - 디바이스가 NTP를 사용하여 management center에서 시간을 수신하도록 클러스터의 플랫폼 설정 정책이 구성된 경우 디바이스를 로컬 시간 관리로 되돌립니다.
 - 구성을 그대로 유지하므로 클러스터가 트래픽을 계속 처리합니다.
- NAT 및 VPN, ACL 및 인터페이스 구성과 같은 정책은 그대로 유지됩니다.

클러스터를 동일하거나 다른 management center에 다시 등록하면 설정이 제거되므로 클러스터는 이 시점에서 트래픽 처리를 중지합니다. 클러스터 구성은 그대로 유지되므로 클러스터 전체를 추가할 수 있습니다. 등록 시 액세스 제어 정책을 선택할 수 있지만, 등록 후에 다른 정책을 다시 적용하고 구성을 구축해야만 트래픽을 다시 처리할 수 있습니다.

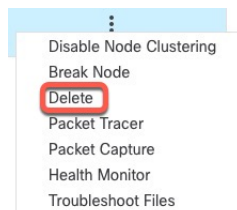
시작하기 전에

이 절차에서는 노드 중 하나에 대한 CLI 액세스가 필요합니다.

프로시저

단계 1 **Devices**(디바이스) > **Device Management**(디바이스 관리)를 선택하고 클러스터 또는 노드로 추가 (⋮)를 클릭하고 **Delete**(삭제)를 선택합니다.

그림 25: 클러스터 또는 노드 삭제



단계 2 클러스터 또는 노드를 삭제하라는 프롬프트가 표시됩니다. **Yes**(예)를 클릭합니다.

단계 3 클러스터 멤버 중 하나를 새 디바이스로 추가하여 클러스터를 새(또는 동일한) management center에 등록할 수 있습니다.

- a) 단일 클러스터 노드의 CLI에 연결하고 **configure manager add** 명령을 사용하여 새 management center를 식별합니다. CLI에서 Threat Defense 관리 인터페이스 수정의 내용을 참조하십시오.
- b) **Devices(디바이스) > Device Management(디바이스 관리)**를 선택한 다음 **Add Device(디바이스 추가)**를 클릭합니다.

클러스터 노드 중 하나만 디바이스로 추가하면 나머지 클러스터 노드가 검색됩니다.

단계 4 삭제된 노드를 다시 추가하려면 [클러스터 노드 조정, 28 페이지](#)의 내용을 참조하십시오.

클러스터 모니터링

management center과 threat defense CLI에서 클러스터를 모니터링할 수 있습니다.

- **Cluster Status(클러스터 상태)** 대화 상자는 **Devices(디바이스) > Device Management > 추가** (아이콘 또는 **Devices(디바이스) > Device Management(디바이스 관리) > Cluster(클러스터) 페이지 > General(일반) 영역 > Cluster Live Status(클러스터 라이브 상태)** 링크에서 제공됩니다.

그림 26: 클러스터 상태

The screenshot shows the 'Cluster Status' interface. At the top, it says 'Overall Status: Cluster has all nodes in sync'. Below this, there are buttons for 'Refresh' and 'Reconcile All', and a search box labeled 'Enter node name'. A table lists the nodes with columns for Status, Device Name, Unit Name, and Chassis URL. The first node is 'Control' with IP 172.16.0.50. The second node has IP 172.16.0.51. Both are in 'In Sync' status.

Status	Device Name	Unit Name	Chassis URL
> In Sync.	172.16.0.50 Control	172.16.0.50	N/A
> In Sync.	172.16.0.51	172.16.0.51	N/A

Dated: 11:52:26 | 20 Dec 2021

Close

제어 노드에는 역할을 식별하는 그래픽 표시기가 있습니다.

클러스터 멤버 상태에는 다음 상태가 포함됩니다.

- 동기화 중 - 노드가 management center에 등록되었습니다.

- 등록 보류 중 - 유닛이 클러스터의 일부이지만 아직 **management center**에 등록되지 않았습니다. 노드 등록에 실패하는 경우, **Reconcile(조정)All(모두)**을 클릭하여 등록을 다시 시도할 수 있습니다.
- 클러스터링이 비활성화됨 - 노드가 **management center**에 등록되었지만, 클러스터의 비활성 멤버입니다. 클러스터링 구성은 나중에 다시 활성화하려는 경우에도 그대로 유지됩니다. 또는 클러스터에서 노드를 삭제할 수 있습니다.
- 클러스터 참가 중... - 노드가 새시의 클러스터에 참가 중이지만 아직 참가가 완료되지 않았습니다. 참가가 끝나면 **management center**로 등록합니다.

각 노드에 대해 요약 또는 기록을 볼 수 있습니다.

그림 27: 노드 요약

Status	Device Name	Unit Name	Chassis URL
In Sync.	172.16.0.50 Control	172.16.0.50	N/A

Summary History

ID: 0 CCL IP: 10.10.10.1
 Site ID: N/A CCL MAC: 6c13.d509.4d9a
 Serial No: FJZ2512139M Module: N/A
 Last join: 05:41:26 UTC Dec 17 2021 Resource: N/A
 Last leave: N/A

그림 28: 노드 기록

Status	Device Name	Unit Name	Chassis URL
In Sync.	172.16.0.50 Control	172.16.0.50	N/A

Summary History

Timestamp	From State	To State	Event
05:56:31 UTC Dec 17 2021	MASTER	MASTER	Event: Cluster new slave enrollment hold for app 1 is relea...
05:56:31 UTC Dec 17 2021	MASTER	MASTER	Event: Cluster new slave enrollment hold for app 1 is relea...
05:56:29 UTC Dec 17 2021	MASTER	MASTER	Event: Cluster new slave enrollment is on hold for app 1 fo...
05:56:29 UTC Dec 17 2021	MASTER	MASTER	Event: Cluster new slave enrollment is on hold for app 1 fo...

- 시스템 (⚙) > **Tasks(작업)** 페이지로 이동합니다.
Tasks(작업) 페이지는 각 노드 등록에 대한 클러스터 등록 작업의 업데이트를 보여줍니다.
- **Devices(디바이스)** > **Device Management(디바이스 관리)** > *cluster_name*.
 디바이스 목록 페이지에서 클러스터를 확장하는 경우, IP 주소 옆에 해당 역할과 함께 표시되는 제어 노드를 포함하여 모든 멤버 노드를 볼 수 있습니다. 아직 등록 중인 로드는 로딩 아이콘이 표시됩니다.
- **show cluster {access-list [acl_name] | conn [count] | cpu [usage] | history | interface-mode | memory | resource usage | service-policy | traffic | xlate count}**

전체 클러스터에 대한 집계된 데이터 또는 다른 정보를 보려면 **show cluster** 명령을 사용합니다.

- **show cluster info** [**auto-join** | **clients** | **conn-distribution** | **flow-mobility counters** | **goid** [*options*] | **health** | **incompatible-config** | **loadbalance** | **old-members** | **packet-distribution** | **trace** [*options*] | **transport** { **asp** | **cp**}]

클러스터 정보를 보려면 **show cluster info** 명령을 사용합니다.

클러스터 상태 모니터 대시보드

클러스터 상태 모니터

threat defense가 클러스터의 제어 노드인 경우 management center는 디바이스 메트릭 데이터 컬렉터에서 다양한 메트릭을 주기적으로 수집합니다. 클러스터 상태 모니터는 다음 구성 요소로 이루어집니다.

- 대시보드 개요 - 클러스터 토폴로지, 클러스터 통계 및 메트릭 차트에 대한 정보를 표시합니다.
 - 토폴로지 섹션에는 클러스터의 라이브 상태, 개별 위협 방어 상태, 위협 방어 노드 유형(제어 노드 또는 데이터 노드) 및 디바이스의 상태가 표시됩니다. 디바이스의 상태는 *Disabled*(비활성화됨)(디바이스가 클러스터에서 나갈 때), *Added out of box*(퍼블릭 클라우드 클러스터에서 management center에 속하지 않는 추가 노드) 또는 *Normal*(노드의 이상적인 상태)일 수 있습니다.
 - 클러스터 통계 섹션에는 CPU 사용량, 메모리 사용량, 입력 속도, 출력 속도, 활성 연결 및 NAT 변환과 관련된 클러스터의 현재 메트릭이 표시됩니다.



참고 CPU 및 메모리 메트릭은 데이터 플레인 및 Snort 사용량의 개별 평균을 표시합니다.

- CPU Usage(CPU 사용량), Memory Usage(메모리 사용량), Throughput(처리량) 및 Connections(연결)와 같은 메트릭 차트는 지정된 기간 동안의 클러스터 통계를 도식적으로 표시합니다.
- 부하 분포 대시보드 - 클러스터 노드 전체의 부하 분포를 다음 두 가지 위젯으로 표시합니다:
 - **Distribution**(배포) 위젯은 클러스터 노드 전체에서 시간 범위의 평균 패킷 및 연결 분포를 표시합니다. 이 데이터는 노드에서 부하가 분산되는 방식을 나타냅니다. 이 위젯을 사용하면 부하 분포의 이상을 쉽게 식별하고 수정할 수 있습니다.
 - **Node Statistics**(노드 통계) 위젯은 노드 레벨 메트릭을 테이블 형식으로 표시합니다. 클러스터 노드 전체에서 CPU 사용량, 메모리 사용량, 입력 속도, 출력 속도, 활성 연결 및 NAT 변환에 대한 메트릭 데이터를 표시합니다. 이 테이블 보기를 사용하면 데이터의 상관관계를 파악하고 불일치를 쉽게 식별할 수 있습니다.

- **Member Performance(멤버 성능) 대시보드** - 클러스터 노드의 현재 메트릭을 표시합니다. 선택기를 사용하여 노드를 필터링하고 특정 노드의 세부 정보를 볼 수 있습니다. 메트릭 데이터에는 CPU 사용량, 메모리 사용량, 입력 속도, 출력 속도, 활성 연결 및 NAT 변환이 포함됩니다.
- **CCL 대시보드** - 클러스터 제어 링크 데이터, 즉 입력 및 출력 속도를 그래픽으로 표시합니다.
- **문제 해결 및 링크** - 자주 사용하는 문제 해결 주제 및 절차에 대한 편리한 링크를 제공합니다.
- **시간 범위** - 다양한 클러스터 메트릭 대시보드 및 위젯에 표시되는 정보를 제한하기 위한 조정 가능한 시간 창입니다.
- **사용자 지정 대시보드** - 클러스터 전체 메트릭 및 노드 레벨 메트릭 모두에 대한 데이터를 표시합니다. 그러나 노드 선택은 위협 방어 메트릭에만 적용되며 노드가 속한 전체 클러스터에는 적용되지 않습니다.

클러스터 상태 보기

이 절차를 수행하려면 관리자, 유지 보수 또는 보안 분석가 사용자여야 합니다.

클러스터 상태 모니터는 클러스터와 해당 노드의 상태에 대한 자세한 보기를 제공합니다. 이 클러스터 상태 모니터는 대시보드 어레이에서 클러스터의 상태 및 추세를 제공합니다.

시작하기 전에

- **management center**에서 하나 이상의 디바이스에서 클러스터를 생성했는지 확인합니다.

프로시저

단계 1 시스템 (⚙) > **Health(상태)** > **Monitor(모니터)**을(를) 선택합니다.

Monitoring(모니터링) 탐색 창을 사용하여 노드별 상태 모니터에 액세스합니다.

단계 2 디바이스 목록에서 **Expand(확장)** (➤) 및 **Collapse(축소)** (▼)를 클릭하여 관리되는 클러스터 디바이스 목록을 확장하고 축소합니다.

단계 3 클러스터 상태 통계를 보려면 클러스터 이름을 클릭합니다. 클러스터 모니터는 기본적으로 사전 정의된 여러 대시보드에서 상태 및 성능 메트릭을 보고합니다. 메트릭 대시보드에는 다음이 포함됩니다.

- **개요** - 노드, CPU, 메모리, 입출력 속도, 연결 통계, NAT 변환 정보 등 미리 정의된 다른 대시보드의 주요 메트릭을 강조 표시합니다.
- **Load Distribution(로드 분포)** - 클러스터 노드 전체의 트래픽 및 패킷 분포입니다.
- **Member Performance(멤버 성능)** - CPU 사용량, 메모리 사용량, 입력 처리량, 출력 처리량, 활성 연결 및 NAT 변환에 대한 노드 레벨 통계.
- **CCL** - 인터페이스 상태 및 집계 트래픽 통계

레이블을 클릭하여 다양한 메트릭 대시보드를 탐색할 수 있습니다. 지원되는 클러스터 메트릭의 전체 목록은 [Cisco Secure Firewall Threat Defense 상태 메트릭](#)을 참고하십시오.

단계 4 오른쪽 상단의 드롭다운에서 시간 범위를 설정할 수 있습니다. 시간 범위는 지난 시간처럼 짧은 기간(기본값) 또는 지난 주처럼 긴 기간을 반영할 수 있습니다. 드롭다운에서 **Custom**(사용자 지정)을 선택하여 사용자 지정 시작 및 종료 날짜를 설정합니다.

새로 고침 아이콘을 클릭하여 자동 새로 고침을 5분으로 설정하거나 자동 새로 고침을 해제합니다.

단계 5 선택한 시간 범위와 관련하여 추세 그래프에서 구축 오버레이를 보려면 구축 아이콘을 클릭합니다. 구축 아이콘은 선택한 시간 범위 동안의 구축 수를 나타냅니다. 세로 줄은 구축 시작 및 종료 시간을 나타냅니다. 다수의 구축이 있는 경우 여러 대역/라인이 나타납니다. 점선 위에 있는 아이콘을 클릭하여 구축 세부 사항을 확인합니다.

단계 6 (노드별 상태 모니터의 경우) 페이지 상단에서 디바이스 이름의 바로 오른쪽에 있는 알림에서 노드의 **Health Alerts**(상태 알림)를 확인합니다.

Health Alerts(상태 알림) 위에 포인터를 올려놓으면 노드의 상태 요약이 표시됩니다. 팝업 윈도우에는 상위 5개 상태 알림의 요약이 잘려서 표시됩니다. 팝업을 클릭하여 상태 알림 요약의 세부사항 보기를 엽니다.

단계 7 (노드별 상태 모니터의 경우) 디바이스 모니터는 기본적으로 사전 정의된 여러 대시보드에서 상태 및 성능 메트릭을 보고합니다. 메트릭 대시보드에는 다음이 포함됩니다.

- **Overview**(개요) - CPU, 메모리, 인터페이스, 연결 통계 등 사전 정의된 다른 대시보드의 주요 메트릭을 강조 표시합니다. 디스크 사용량 및 중요 프로세스 정보도 포함됩니다.
- **CPU** - CPU 사용률(프로세스 및 물리적 코어별 CPU 사용률 포함)
- **메모리**-데이터 플레인 및 Snort 메모리 사용량을 포함한 디바이스 메모리 사용량입니다.
- **Interfaces**(인터페이스) - 인터페이스 상태 및 집계 트래픽 통계
- **Connections**(연결) - 연결 통계(예: 엘리펀트 플로우, 활성 연결, 최대 연결 등) 및 NAT 변환 수.
- **Snort** - Snort 프로세스와 관련된 통계
- **ASP 삭제** - 여러 이유로 인해 삭제된 패킷과 관련된 통계입니다.

레이블을 클릭하여 다양한 메트릭 대시보드를 탐색할 수 있습니다. 지원되는 디바이스 메트릭의 전체 목록은 [Cisco Secure Firewall Threat Defense 상태 메트릭](#)을 참고하십시오.

단계 8 사용 가능한 메트릭 그룹에서 고유한 변수 집합을 작성하여 사용자 지정 대시보드를 생성하려면 상태 모니터의 오른쪽 상단 모서리에 있는 더하기 기호(+)**를** 클릭합니다.

클러스터 전체 대시보드의 경우 **Cluster metric group**(클러스터 메트릭 그룹)을 선택한 다음 메트릭을 선택합니다.

클러스터 메트릭

클러스터 상태 모니터는 클러스터 및 해당 노드와 관련된 통계와 로드 분포, 성능 및 CCL 트래픽 통계의 집계를 추적합니다.

표 2: 클러스터 메트릭

메트릭	설명	형식
CPU	클러스터의 노드에 있는 CPU 메트릭의 평균입니다(데이터 플레인 및 snort에 대해 개별적으로).	백분율
메모리	클러스터의 노드에 있는 메모리 메트릭의 평균입니다(데이터 플레인 및 snort에 대해 개별적으로).	백분율
데이터 처리량	클러스터에 대한 수신 및 발신 데이터 트래픽 통계입니다.	바이트
CCL 처리량	클러스터에 대한 수신 및 발신 CCL 트래픽 통계입니다.	바이트
연결	클러스터의 활성 연결 수입니다.	숫자
NAT 변환	클러스터에 대한 NAT 변환 수.	숫자
배포	초당 클러스터의 연결 분포 수입니다.	숫자
패킷	초당 클러스터의 패킷 배포 수입니다.	숫자

클러스터링에 대한 참조

이 섹션에는 클러스터링이 작동하는 방식에 대한 자세한 정보가 포함되어 있습니다.

위협 방어 기능 및 클러스터링

일부 threat defense 기능은 클러스터링이 지원되지 않으며, 일부 기능은 기본 유닛에서만 지원됩니다. 기타 기능의 경우 올바르게 사용하는 데 필요한 주의 사항이 있을 수 있습니다.

지원되지 않는 기능 및 클러스터링

이러한 기능은 클러스터링을 사용하도록 설정한 경우 구성할 수 없으며 명령이 거부됩니다.



참고 클러스터링으로도 지원되지 않는 FlexConfig 기능(예: WCCP 검사)을 보려면 [ASA 일반 운영 설정 가이드](#)를 참조하십시오. FlexConfig를 사용하면 management center GUI에 없는 여러 ASA 기능을 설정할 수 있습니다. [FlexConfig 정책](#)의 내용을 참조하십시오.

- 원격 액세스 VPN(SSL VPN 및 IPsec VPN)
- DHCP 클라이언트, 서버, 프록시 DHCP 릴레이가 지원됩니다.
- Virtual Tunnel Interface(VTI)
- 고가용성
- 통합 라우팅 및 브리징
- FMC UCAPL/CC 모드

클러스터링을 위한 중앙 집중식 기능

다음 기능은 제어 노드에서만 지원되며 클러스터에 확장되지 않습니다.



참고 중앙 집중식 기능의 트래픽은 클러스터 제어 링크를 통해 멤버 노드에서 제어 노드로 전달됩니다. 리밸런싱 기능을 사용할 경우, 중앙 집중식 기능의 트래픽은 트래픽이 중앙 집중식 기능으로 분류되기 전에 비 제어 노드로 리밸런싱될 수 있습니다. 이렇게 되면 해당 트래픽은 제어 노드로 다시 전송됩니다.

중앙 집중식 기능의 경우 제어 노드에 오류가 발생하면 모든 연결이 취소되며 새 제어 노드에서 연결을 다시 설정해야 합니다.



참고 클러스터링으로도 집중되는 FlexConfig 기능(예: RADIUS 검사)을 보려면 [ASA 일반 운영 설정 가이드](#)를 참조하십시오. FlexConfig를 사용하면 management center GUI에 없는 여러 ASA 기능을 설정할 수 있습니다. [FlexConfig 정책](#)의 내용을 참조하십시오.

- 다음과 같은 애플리케이션 감사:
 - DCERPC
 - ESMTP
 - NetBIOS
 - PPTP
 - RSH
 - SQLNET
 - SUNRPC
 - TFTP
 - XDMCP

- 고정 경로 모니터링

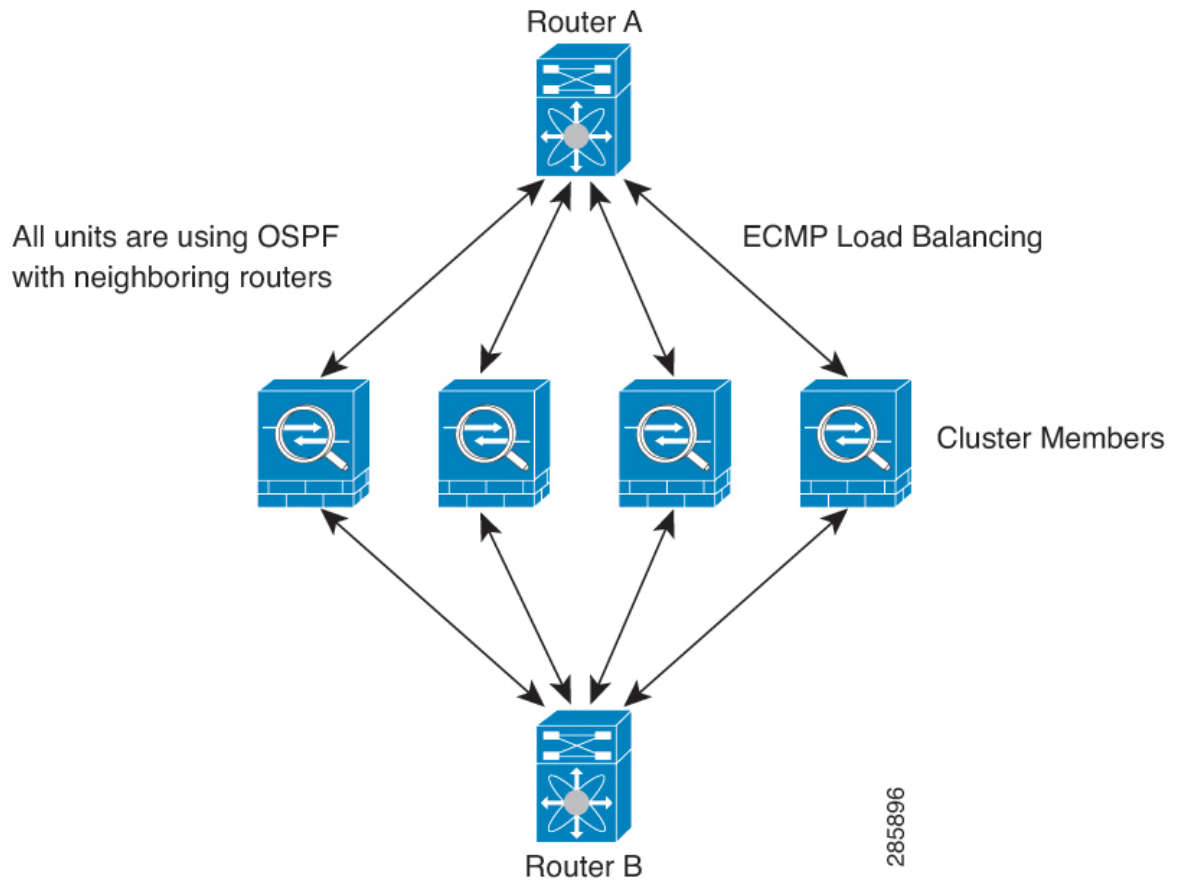
연결 설정 및 클러스터링

연결 제한은 클러스터 전체에서 시행됩니다. 각 노드에는 브로드캐스트 메시지를 기반으로 한 클러스터 전체의 카운터 값이 표시됩니다. 효율성을 고려하여 클러스터 전체에 구성된 연결 제한이 제한수에 정확하게 적용되지 않을 수 있습니다. 각 노드는 언제든지 클러스터 전체 카운터 값을 과대 평가하거나 과소 평가할 수 있습니다. 그러나 로드 밸런싱된 클러스터에서는 시간이 지남에 따라 정보가 업데이트됩니다.

동적 라우팅 및 클러스터링

개별 인터페이스 모드인 경우 각 노드에서는 라우팅 프로토콜을 독립형 라우터로 실행하며, 경로에 대한 정보 학습은 각 노드에서 개별적으로 수행합니다.

그림 29: 개별 인터페이스 모드인 동적 라우팅



위 다이어그램에서 라우터 A는 라우터 B에 각각 노드를 통한 4개의 Equal-Cost 경로가 있다는 정보를 파악합니다. ECMP는 4개 경로 간의 트래픽을 로드 밸런싱하는 데 사용됩니다. 각각의 노드는 외부 라우터와 통신할 경우 다른 라우터 ID를 선택합니다.

라우터 ID에 대한 클러스터 풀을 구성하여 노드마다 개별 라우터 ID를 보유하도록 해야 합니다.

FTP 및 클러스터링

- 다른 클러스터 멤버가 FTP 데이터 채널 및 제어 채널의 흐름을 소유한 경우, 데이터 채널 소유자 유닛에서는 유희 시간 제한 업데이트를 제어 채널 소유자에게 주기적으로 전송하고 유희 시간 제한 값을 업데이트합니다. 그러나 제어 흐름 소유자가 다시 로드되고 제어 흐름이 다시 호스팅된 경우, 부모/자식 흐름 관계가 더 이상 유지되지 않으며 제어 흐름 유희 시간 제한도 업데이트되지 않습니다.

NAT 및 클러스터링

NAT는 클러스터의 전체 처리량에 영향을 미칠 수 있습니다. 로드 밸런싱 알고리즘은 IP 주소와 포트를 기반으로 할 뿐만 아니라 NAT로 인해 인바운드 및 아웃바운드 패킷의 IP 주소 및/또는 포트가 서로 달라질 수 있으므로, 인바운드 및 아웃바운드 NAT 패킷을 클러스터의 다른 threat defense에 전송할 수 있습니다. 패킷이 NAT 소유자가 아닌 threat defense에 전달되면 해당 패킷은 클러스터 제어 링크를 통해 소유자에게 전달되며 이때 클러스터 제어 링크에 매우 많은 양의 트래픽이 발생합니다. 보안 및 정책 확인 결과에 따라 NAT 소유자가 패킷에 대해 연결을 생성하지 않을 수 있으므로 수신 노드는 소유자에 대한 전달 플로우를 생성하지 않습니다.

클러스터링에 NAT를 계속 사용하려면 다음 지침을 숙지하십시오.

- 프록시 ARP 없음 — 개별 인터페이스에서 프록시 ARP 응답은 매핑된 주소에 전송되지 않습니다. 이렇게 되면 인접한 라우터가 클러스터에 더 이상 존재하지 않을 수 있는 ASA와 피어 관계를 유지하지 못하게 됩니다. 업스트림 라우터에는 기본 클러스터 IP 주소를 나타내는 매핑된 주소에 대한 고정 경로 또는 PBR(Object Tracking 포함)이 필요합니다.
- 개별 인터페이스에 인터페이스 PAT 없음 — 개별 인터페이스에는 인터페이스 PAT가 지원되지 않습니다.
- 포트 블록 할당이 있는 PAT - 이 기능에 대한 다음 지침을 참조하십시오.
 - 호스트당 최대 제한은 클러스터 전체 제한이 아니며 각 노드에서 개별적으로 적용됩니다. 호스트당 최대 제한이 1로 구성된 3-노드 클러스터에서 호스트의 트래픽이 3개 노드 모두에 로드 밸런싱되는 경우 각 노드에 하나씩 3개의 블록이 할당될 수 있습니다.
 - 백업 풀의 백업 노드에서 생성된 포트 블록은 호스트당 최대 제한을 적용할 때 고려되지 않습니다.
 - 완전히 새로운 IP 범위로 PAT 풀을 수정하는 즉석 PAT 규칙 수정을 수행할 경우, 새 풀이 작동하게 되는 동안 여전히 전환 중이던 xlate 백업 요청에 대해 xlate 백업 생성이 실패하게 됩니다. 이러한 동작은 포트 블록 할당 기능과 관련이 없으며, 풀이 분산되고 트래픽이 클러스터 노드 전체에서 부하 분산되는 클러스터 구축 과정에서만 발생하는 일시적인 PAT 풀 문제입니다.
 - 클러스터에서 작업할 때는 단순히 블록 할당 크기를 변경할 수 없습니다. 새 크기는 클러스터에서 각 디바이스를 다시 로드한 후에만 적용됩니다. 각 디바이스를 다시 로드하지 않으려면 모든 블록 할당 규칙을 삭제하고 해당 규칙과 관련된 모든 xlate를 지우는 것이 좋습니다. 그런 다음 블록 크기를 변경하고 블록 할당 규칙을 다시 생성할 수 있습니다.

- 동적 PAT에 대한 NAT 풀 주소 분산 - PAT 풀을 구성하면 클러스터는 풀의 각 IP 주소를 포트 블록으로 나눕니다. 기본적으로 각 블록은 512포트이지만 포트 블록 할당 규칙을 구성하는 경우에는 블록 설정이 대신 사용됩니다. 이러한 블록은 클러스터의 노드 간에 균등하게 분산되므로 각 노드에는 PAT 풀의 각 IP 주소에 대해 하나 이상의 블록이 있습니다. 따라서 예상되는 PAT 처리된 연결 수에 충분한 경우 클러스터의 PAT 풀에 IP 주소를 하나만 포함할 수 있습니다. PAT 풀 NAT 규칙에 예약된 포트 1~1023을 포함하도록 옵션을 구성하지 않는 한 포트 블록은 1024~65535 포트 범위를 포함합니다.
- 여러 규칙에서 PAT 풀 재사용 - 여러 규칙에서 동일한 PAT 풀을 사용하려면 규칙에서 인터페이스 선택에 주의해야 합니다. 모든 규칙에서 특정 인터페이스를 사용하거나 또는 모든 규칙에서 "any(임의의)"를 사용해야 합니다. 규칙 전체에서 특정 인터페이스와 "any(임의의)"를 혼합할 수 없거나, 시스템에서 클러스터의 오른쪽 노드에 대한 반환 트래픽을 일치시키지 못할 수 있습니다. 규칙 당 고유한 PAT 풀을 사용하는 것은 가장 신뢰할 수 있는 옵션입니다.
- 라운드 로빈 없음 — 클러스터링에서는 PAT 풀을 위한 라운드 로빈을 지원하지 않습니다.
- 확장 PAT 없음 - 클러스터링에서 확장 PAT가 지원되지 않습니다.
- 제어 노드에 의해 관리되는 동적 NAT xlate — 제어 노드에서는 xlate 테이블을 유지하고 데이터 노드에 복제합니다. 동적 NAT가 필요한 연결이 데이터 노드에 전달되고 xlate가 테이블에 없을 경우, 제어 노드에서 xlate를 요청합니다. 데이터 노드에서는 이 연결을 소유합니다.
- 오래된 xlates - 연결 소유자의 xlate 유효 시간이 업데이트되지 않습니다. 따라서 유효 시간이 유효 시간 제한을 초과할 수 있습니다. refcnt가 0인 구성된 시간 초과 값보다 큰 유효 타임 값은 오래된 xlate를 나타냅니다.
- 다음을 검사할 수 있는 고정 PAT 없음
 - FTP
 - RSH
 - SQLNET
 - TFTP
 - XDMCP
 - SIP
- 10,000개가 넘는 매우 많은 NAT 규칙이 있는 경우 디바이스 CLI에서 **asp rule-engine transactional-commit nat** 명령을 사용하여 트랜잭션 커밋 모델을 활성화해야 합니다. 그렇지 않으면 노드가 클러스터에 조인하지 못할 수 있습니다.

SIP 검사 및 클러스터링

로드 밸런싱으로 인해 모든 노드에서 제어 플로우를 만들 수 있지만 하위 데이터 플로우는 동일한 노드에 상주해야 합니다.

SNMP 및 클러스터링

SNMP 에이전트에서는 진단 인터페이스 로컬 IP 주소로 각각의 개별 threat defense를 폴링합니다. 클러스터의 통합 데이터는 폴링할 수 없습니다.

SNMP 폴링에는 기본 클러스터 IP 주소가 아닌 로컬 주소를 항상 사용해야 합니다. SNMP 에이전트에서 기본 클러스터 IP 주소를 폴링하면서 새 제어 노드가 선택된 경우, 새 제어 노드에 대한 폴링이 이루어지지 않습니다.

클러스터링과 함께 SNMPv3를 사용할 때 초기 클러스터 형성 후 새 클러스터 노드를 추가하면 SNMPv3 사용자가 새 노드에 복제되지 않습니다. 사용자를 제거하고 다시 추가한 다음 사용자가 새 노드에 복제하도록 강제로 구성을 재구축해야 합니다.

시스템 로그 및 클러스터링

- 클러스터의 각 노드에서는 고유한 syslog 메시지를 생성합니다. 각 노드에서 syslog 메시지 헤더 필드에 동일하거나 다른 디바이스 ID를 사용하도록 로깅을 구성할 수 있습니다. 예를 들어, 호스트 이름 구성은 클러스터의 모든 노드에 의해 복제 및 공유됩니다. 호스트 이름을 디바이스 ID로 사용하도록 로깅을 구성할 경우, 모든 노드에서는 단일 노드에서 생성된 것처럼 보이는 syslog 메시지를 생성합니다. 클러스터 부트스트랩 구성에 할당된 로컬-노드 이름을 디바이스 ID로 사용하도록 로깅을 구성할 경우, syslog 메시지는 다른 노드에서 생성된 것처럼 보입니다.

Cisco TrustSec 및 클러스터링

제어 노드에서만 보안 그룹 태그(SGT) 정보를 학습합니다. 그런 다음 제어 노드에서는 SGT를 데이터 노드에 제공하며, 데이터 노드에서는 보안 정책을 기준으로 SGT의 일치 여부를 결정할 수 있습니다.

VPN 및 클러스터링

VPN 기능은 마스터 노드에만 제한되며 클러스터 고가용성 기능을 사용하지 않습니다. 제어 노드에 오류가 발생할 경우, 모든 기존 VPN 연결이 손실되며 VPN 사용자에게는 서비스 중단 메시지가 표시됩니다. 새 제어 노드가 선택되면 VPN 연결을 다시 설정해야 합니다.

PBR 또는 ECMP를 사용할 경우 개별 인터페이스에 연결하려면 항상 로컬 주소가 아닌 기본 클러스터 IP 주소에 연결해야 합니다.

VPN 관련 키 및 인증서는 모든 노드에 복제됩니다.



참고 원격 액세스 VPN은 클러스터링으로 지원되지 않습니다.

성능 확장 요소

클러스터에 여러 유닛을 결합할 경우 총 클러스터 성능을 대략 최대 결합 처리량의 약 80%로 예측할 수 있습니다.

예를 들어 모델이 단독으로 실행될 때 약 10Gbps의 트래픽을 처리할 수 있는 경우, 8개 유닛으로 구성된 클러스터의 경우 최대 통합 처리량은 80Gbps(8개 유닛 x 10Gbps)의 약 80%인 64Gbps가 됩니다.

제어 노드 선택

클러스터의 노드는 클러스터 제어 링크로 통신을 수행하여 다음과 같은 방식으로 제어 노드를 선택합니다.

1. 노드에 클러스터링을 사용할 경우(또는 이미 사용 설정된 클러스터링을 처음 시작할 경우), 선택 요청이 3초마다 전송됩니다.
2. 다른 노드의 우선순위가 더 높을 경우 해당 노드가 선택 요청에 응답하게 됩니다. 우선순위는 1에서 100까지 설정되며 1이 가장 높은 우선순위입니다.
3. 45초 후에 우선순위가 더 높은 다른 노드에서 응답을 받지 못한 노드는 제어 노드가 됩니다.



참고 가장 우선순위가 높은 노드가 공동으로 여러 개인 경우, 클러스터 노드 이름과 일련 번호를 사용하여 제어 노드를 결정합니다.

4. 노드가 우선순위가 더 높은 클러스터에 참가한다고 해서 해당 노드가 자동으로 제어 노드가 되는 것은 아닙니다. 기존 제어 노드는 응답이 중지되지 않는 한 항상 제어 노드로 유지되며 응답이 중지될 때에 새 제어 노드가 선택됩니다.
5. 제어 노드가 일시적으로 여러 개 있는 "스플릿 브레인" 시나리오에서는 우선 순위가 가장 높은 노드가 역할을 유지하는 반면 다른 노드는 데이터 노드 역할로 돌아갑니다.



참고 노드를 수동으로 강제 변경하여 제어 노드가 되도록 할 수 있습니다. 중앙 집중식 기능의 경우 제어 노드를 강제로 변경하면 모든 연결이 취소되며 새 제어 노드에서 연결을 다시 설정해야 합니다.

클러스터 내의 고가용성

클러스터링에서는 노드 및 인터페이스의 상태를 모니터링하고 노드 간의 연결 상태를 복제하여 고가용성을 제공합니다.

노드 상태 모니터링

각 노드는 클러스터 제어 링크를 통해 브로드 캐스트 heartbeat 패킷을 주기적으로 전송합니다. 제어 노드가 구성 가능한 시간 초과 기간 내에 데이터 유닛에서 heartbeat 패킷 또는 기타 패킷을 수신하지 않는 경우, 제어 노드는 클러스터에서 데이터 노드를 제거합니다. 데이터 노드가 제어 노드에서 패킷을 수신하지 않으면 나머지 노드에서 새 제어 노드가 선택됩니다.

네트워크 장애로 인해 노드가 실제로 장애가 발생한 것이 아니라 클러스터 제어 링크를 통해 노드가 서로 연결할 수 없는 경우, 클러스터는 격리된 데이터 노드가 자체 제어 노드를 선택하는 "스플릿 브

레인" 시나리오로 전환될 수 있습니다. 예를 들어 두 클러스터 위치 간에 라우터가 실패하면 위치 1의 원래 제어 노드가 클러스터에서 위치 2 데이터 노드를 제거합니다. 한편, 위치 2의 노드는 자체 제어 노드를 선택하고 자체 클러스터를 구성합니다. 이 시나리오에서는 비대칭 트래픽이 실패할 수 있습니다. 클러스터 제어 링크가 복원되면 우선 순위가 더 높은 제어 노드가 제어 노드의 역할을 유지합니다.

인터페이스 모니터링

각 노드에서는 사용 중인 모든 명명된 하드웨어 인터페이스의 링크 상태를 모니터링하며 상태 변경 사항을 제어 노드에 보고합니다.

모든 물리적 인터페이스가 모니터링됩니다. 명명된 인터페이스만 모니터링할 수 있습니다. 선택적으로 인터페이스별 모니터링을 비활성화할 수 있습니다.

노드의 모니터링된 인터페이스에 장애가 발생하면 클러스터에서 해당 노드가 제거됩니다. 노드는 500밀리초 후에 제거됩니다.

실패 이후 상태

클러스터의 노드에 오류가 발생할 경우, 해당 노드에서 호스팅하는 연결이 다른 노드로 원활하게 전송되며 트래픽에 대한 상태 정보가 제어 노드의 클러스터 제어 링크를 통해 공유됩니다.

제어 노드에 장애가 발생할 경우, 우선순위가 가장 높은(숫자가 가장 낮은) 클러스터의 다른 멤버가 제어 노드가 됩니다.

threat defense는 실패 이벤트에 따라 클러스터에 다시 참가하려고 시도합니다.



참고 threat defense가 비활성화되고 클러스터에 자동으로 다시 조인하지 못할 경우, 모든 데이터 인터페이스가 종료되며 관리/진단 인터페이스에서만 트래픽을 주고받을 수 있습니다.

클러스터 다시 참가

클러스터 멤버가 클러스터에서 제거된 후 해당 멤버가 클러스터에 다시 참가할 수 있는 방법은 처음에 제거된 이유에 따라 결정됩니다.

- 최초 가입 시 오류가 발생한 클러스터 제어—클러스터 제어 링크의 문제를 해결한 다음 클러스터링을 다시 활성화하여 수동으로 클러스터를 다시 가입시켜야 합니다.
- 클러스터 가입 후 클러스터 제어 링크 장애 —FTD에서는 자동으로 5분마다 무기한으로 다시 가입하려고 시도합니다.
- 데이터 인터페이스 오류 — threat defense에서는 5분에 다시 참가를 시도하며 그다음에는 10분, 마지막으로 20분에 참가를 시도합니다. 20분 후에도 참가가 이루어지지 않을 경우 threat defense에서는 클러스터링을 비활성화합니다. 데이터 인터페이스의 문제를 해결한 다음 수동으로 클러스터링을 활성화해야 합니다.
- 노드 오류 — 노드 상태 검사 오류로 인해 클러스터에서 노드가 제거된 경우, 클러스터에 다시 참가할 수 있는지 여부는 오류의 원인에 따라 결정됩니다. 예를 들어, 일시적인 정전이 발생한

경우 클러스터 제어 링크가 작동 상태이면 전원을 다시 가동할 때 노드가 클러스터에 다시 참가할 수 있습니다. threat defense 애플리케이션은 5초마다 클러스터에 다시 참가하려고 시도합니다.

- 내부 오류 — 내부 장애 포함: 애플리케이션 동기화 시간 초과, 일치하지 않는 애플리케이션 상태 등이 있습니다.
- 실패한 구성 구축-FMC에서 새 구성을 구축하는 경우 일부 클러스터 멤버에서는 구축이 실패하지만 다른 클러스터 멤버에서는 성공할 경우 실패한 노드는 클러스터에서 제거됩니다. 문제를 해결한 후 클러스터링을 다시 사용하도록 설정하여 클러스터에 수동으로 다시 참가해야 합니다. 제어 노드에서 구축이 실패하면 구축이 롤백되고 멤버가 제거되지 않습니다. 모든 데이터 노드에서 구축이 실패하면 구축이 롤백되고 멤버가 제거되지 않습니다.

데이터 경로 연결 상태 복제

모든 연결마다 클러스터 내에 하나의 소유자 및 최소 하나의 백업 소유자가 있습니다. 백업 소유자는 장애 발생 시 연결을 인계받는 대신 TCP/UDP 상태 정보를 저장하므로, 장애가 발생할 경우 연결이 새로운 소유자에게 원활하게 전송될 수 있습니다. 백업 소유자는 일반적으로 관리자이기도 합니다.

일부 트래픽의 경우 TCP 또는 UDP 레이어 상위에 대한 상태 정보가 필요합니다. 클러스터링 지원에 대해 알아보거나 이러한 종류의 트래픽에 대한 지원이 부족한 경우 다음 표를 참조하십시오.

표 3: 클러스터 전반에 걸쳐 복제된 기능

트래픽	상태 지원	참고
가동 시간	예	시스템 가동 시간을 추적합니다.
ARP 테이블	예	—
MAC 주소 테이블	예	—
사용자 ID	예	—
IPv6 네이버 데이터베이스	예	—
동적 라우팅	예	—
SNMP 엔진 ID	아니요	—

클러스터에서 연결을 관리하는 방법

클러스터의 여러 노드에 대한 연결을 로드 밸런싱할 수 있습니다. 연결 역할은 정상적인 작동이 이루어지고 있고 가용성이 높은 상황에서 연결을 처리하는 방법을 결정합니다.

연결 역할

각 연결에 대해 정의된 다음 역할을 참조하십시오.

- 소유자 - 일반적으로 연결을 가장 처음 수신하는 노드입니다. 소유자 유닛에서는 TCP 상태를 유지하고 패킷을 처리합니다. 연결이 하나인 경우 소유자 유닛도 1개뿐입니다. 원래 소유자가 실패하고 새 노드가 연결에서 패킷을 수신하면, 관리자는 해당 노드로부터 새 소유자를 선택합니다.
- 백업 소유자 - 장애가 발생할 경우 연결이 새로운 소유자에게 원활하게 전송될 수 있도록 소유자로부터 수신한 TCP/UDP 상태 정보를 저장하는 노드입니다. 백업 소유자는 장애 발생 시 연결을 승계할 수 없습니다. 소유자를 사용할 수 없는 경우, 연결에서 (로드 밸런싱을 기준으로) 패킷을 받을 첫 번째 노드가 백업 소유자에 관련 상태 정보를 문의하면 해당 백업 소유자가 새로운 소유자가 될 수 있습니다.

관리자(아래 설명 참조)는 소유자와 같은 노드가 아니라면 백업 소유자로도 사용됩니다. 소유자가 자신을 관리자라 선택하면 별도의 백업 소유자가 선택됩니다.

Firepower 9300의 클러스터링(새시 하나에 클러스터 노드가 3개까지 포함될 수 있음)에서 백업 소유자가 소유자와 같은 새시에 있으면 새시 장애로부터 플로우를 보호하기 위해 다른 새시에서 추가 백업 소유자가 선택됩니다.

- 관리자 - 전달자의 소유자 조회 요청을 처리하는 노드입니다. 소유자가 새 연결을 수신할 경우, 소유자 노드에서는 소스/대상 IP 주소와 포트의 해시를 기준으로 관리자를 선택하며 관리자에 메시지를 전송하여 새 연결을 등록합니다(아래에서 ICMP 해시 세부 정보 참조). 패킷이 소유자가 아닌 다른 노드에 전달될 경우, 해당 노드는 관리자에 어떤 노드가 소유자인지 조회하여 패킷이 전달될 수 있도록 합니다. 연결이 하나인 경우 관리자 유닛도 1개뿐입니다. 관리자가 실패하면 소유자는 새 관리자를 선택합니다.

관리자는 소유자와 같은 노드가 아니면 백업 소유자로도 사용됩니다(위의 설명 참조). 소유자가 자신을 디렉터로 선택하면 별도의 백업 소유자가 선택됩니다.

ICMP/ICMPv6 해시 세부 정보:

- 에코 패킷의 경우 소스 포트는 ICMP 식별자이고, 대상 포트는 0입니다.
- 응답 패킷의 경우 소스 포트는 0이고, 대상 포트는 ICMP 식별자입니다.
- 기타 패킷의 경우 소스 및 대상 포트가 모두 0입니다.

- 전달자 — 패킷을 소유자에 전달하는 노드입니다. 소유하지 않은 연결 패킷이 전달자 유닛에 수신될 경우, 전달자 유닛에서는 소유자 유닛의 관리자를 조회한 다음 이러한 연결을 수신하는 기타 모든 패킷의 소유자에 대한 흐름을 설정합니다. 관리자 유닛은 전달자가 될 수도 있습니다. 전달자 유닛에서 SYN-ACK 패킷을 수신할 경우, 패킷의 SYN 쿠키에서 소유자를 직접 파생할 수 있으므로 관리자 유닛에 조회하지 않아도 됩니다. (TCP 시퀀스 임의 설정을 비활성화한 경우 SYN 쿠키는 사용되지 않으며, 책임자에게 쿼리해야 합니다.) DNS 및 ICMP 같이 짧은 흐름의 경우 쿼리 대신 전달자가 책임자에게 패킷을 즉시 전송하고 책임자가 소유자에게 전송합니다. 하나의 연결에 여러 개의 전달자 유닛이 있을 수 있습니다. 가장 효율적인 처리량 목표를 실현하려면 전달자가 없고 연결의 모든 패킷이 소유자 유닛에 전송되는 우수한 로드 밸런싱 방법을 사용합니다.



참고 클러스터링을 사용할 때는 TCP 시퀀스 임의 설정을 비활성화하지 않는 것이 좋습니다. SYN/ACK 패킷이 삭제될 수 있으므로 일부 TCP 세션이 설정되지 않을 가능성이 적습니다.

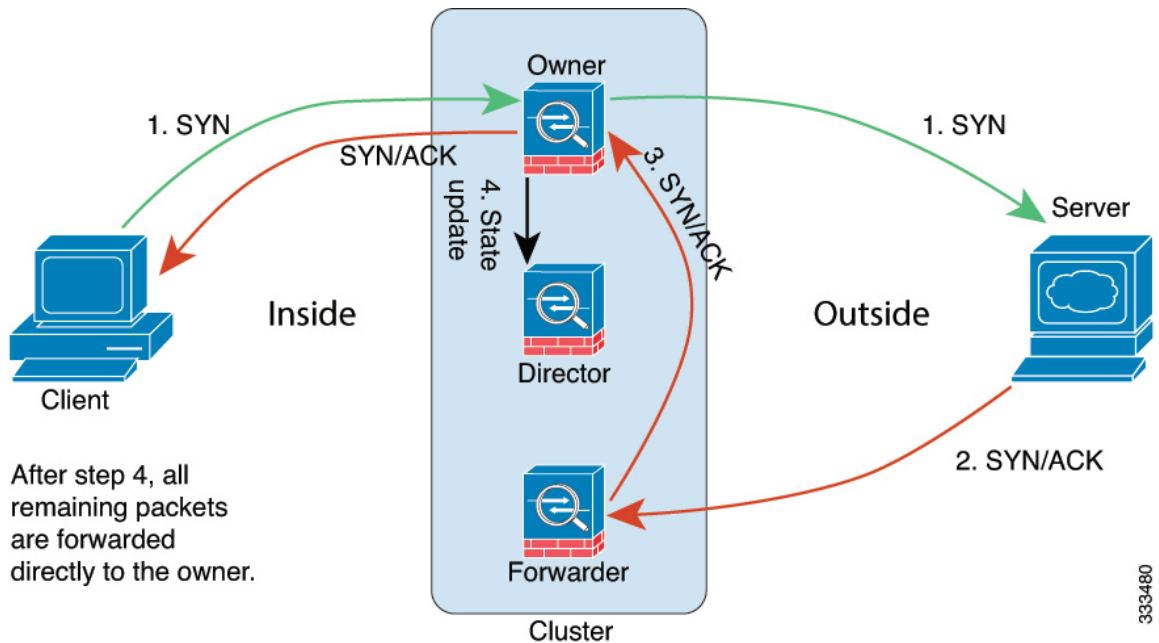
- 프래그먼트 소유자 - 프래그먼트화된 패킷의 경우 프래그먼트를 수신하는 클러스터 노드가 프래그먼트 소스 IP 주소, 대상 IP 주소 및 패킷 ID의 해시를 사용하여 프래그먼트 소유자를 결정합니다. 그런 다음 모든 프래그먼트가 클러스터 제어 링크를 통해 프래그먼트 소유자에게 전달됩니다. 첫 번째 프래그먼트만 스위치 로드 밸런싱 해시에 사용되기 때문에 프래그먼트는 다른 클러스터 노드로 로드 밸런싱될 수 있습니다. 다른 프래그먼트는 소스 및 대상 포트를 포함하지 않으며 다른 클러스터 노드에 로드 밸런싱될 수 있습니다. 프래그먼트 소유자는 패킷을 일시적으로 리어셈블하므로 소스/대상 IP 주소 및 포트의 해시를 기반으로 디렉터를 확인할 수 있습니다. 새 연결인 경우 프래그먼트 소유자가 연결 소유자로 등록됩니다. 기존 연결인 경우 프래그먼트 소유자는 클러스터 제어 링크를 통해 모든 프래그먼트를 제공된 연결 소유자에게 전달합니다. 그러면 연결 소유자가 모든 프래그먼트를 리어셈블합니다.

새 연결 소유권

로드 밸런싱을 통해 클러스터의 노드에 새 연결이 전송될 경우, 해당 노드에서는 연결의 양방향 모두 소유합니다. 다른 노드에 연결 패킷이 전송될 경우, 해당 패킷은 클러스터 제어 링크를 통해 소유자 노드에 전달됩니다. 다른 노드에 반대 방향의 흐름이 전송될 경우, 이는 원래 노드로 다시 리디렉션됩니다.

TCP에 대한 샘플 데이터 플로우

다음 예에는 새 연결을 설정하는 방법이 나와 있습니다.



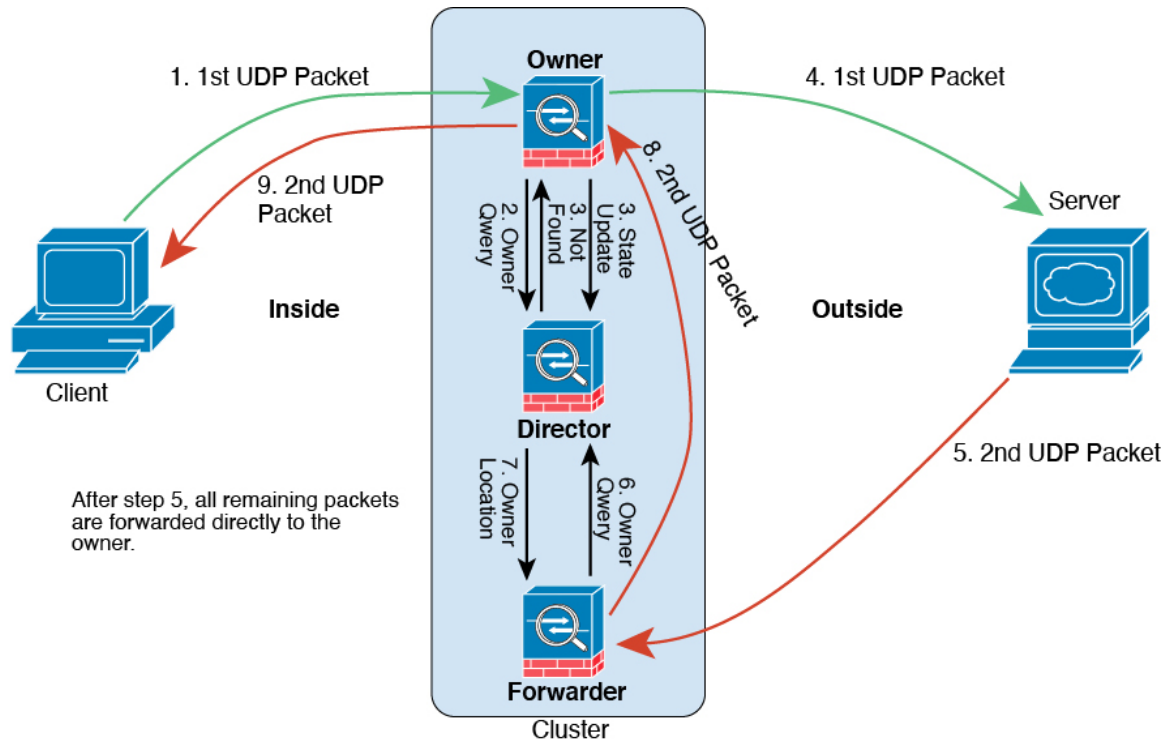
333480

1. SYN 패킷은 클라이언트에서 시작되고 threat defense에 전달(로드 밸런싱 방법을 기준으로)되며, 이 유닛이 소유자 유닛이 됩니다. 소유자 유닛에서는 흐름을 생성하고, 소유자 정보를 SYN 쿠키로 인코딩하며, 패킷을 서버에 전달합니다.
2. SYN-ACK 패킷은 서버에서 시작되고 다른 threat defense에 전달(로드 밸런싱 방법을 기준으로)됩니다. 이 threat defense는 전달자 유닛입니다.
3. 전달자 유닛에서는 연결을 소유하지 않으므로 SYN 쿠키에서 소유자 정보를 디코딩하고, 소유자에 대한 전달 흐름을 생성하며, SYN-ACK를 소유자 유닛에 전달합니다.
4. 소유자 유닛에서는 관리자 유닛에 상태 업데이트를 보내고, SYN-ACK를 클라이언트에 전달합니다.
5. 관리자 유닛에서는 소유자 유닛을 통해 상태 업데이트를 수신하고, 소유자에 대한 흐름을 생성하며, TCP 상태 정보는 물론 소유자를 기록합니다. 관리자 유닛은 연결의 백업 소유자 역할을 수행합니다.
6. 전달자 유닛에 전달된 모든 후속 패킷은 소유자 유닛에 전달됩니다.
7. 패킷이 추가 노드에 전달된 경우, 관리자에 쿼리하고 플로우를 설정합니다.
8. 플로우 결과의 상태가 변경되면 소유자 유닛과 관리자 유닛의 상태도 업데이트됩니다.

ICMP 및 UDP의 샘플 데이터 플로우

다음 예에는 새 연결을 설정하는 방법이 나와 있습니다.

1. 그림 30: ICMP 및 UDP 데이터 플로우



첫 번째 UDP 패킷은 클라이언트에서 시작되고 (로드 밸런싱 방법을 기준으로) threat defense에 전달됩니다.

2. 첫 번째 패킷을 수신한 노드는 소스/대상 IP 주소 및 포트의 해시를 기반으로 선택된 관리자 노드에 쿼리합니다.
3. 관리자는 기존 플로우를 찾지 못하고 관리자 플로우를 생성하며 이전 노드로 패킷을 다시 전달합니다. 즉, 관리자가 이 플로우의 소유자를 선택했습니다.
4. 소유자가 플로우를 생성하고 관리자에게 상태 업데이트를 보내고 서버에 패킷을 전달합니다.
5. 두 번째 UDP 패킷은 서버에서 시작되어 전달자에게 전달됩니다.
6. 전달자는 관리자에게 소유권 정보를 쿼리합니다. DNS와 같이 짧은 플로우의 경우 쿼리하는 대신 전달자가 관리자에게 패킷을 즉시 전송하고 관리자가 소유자에게 전송합니다.
7. 관리자는 전달자에게 소유권 정보를 회신합니다.
8. 전달자는 전달 플로우를 생성하여 소유자 정보를 기록하고 소유자에게 패킷을 전달합니다.
9. 소유자는 패킷을 클라이언트에 전달합니다.

프라이빗 클라우드의 Threat Defense 가상 클러스터링 기록

기능	버전	세부 사항
클러스터 상태 모니터링 설정	7.3	<p>이제 클러스터 상태 모니터링 설정을 편집할 수 있습니다.</p> <p>신규/수정된 화면: Devices(디바이스) > Device Management(디바이스 관리) > Cluster(클러스터) > Cluster Health Monitor Settings(클러스터 상태 모니터링 설정)</p> <p>참고 이전에 FlexConfig를 사용하여 이러한 설정을 구성한 경우 구축하기 전에 FlexConfig 구성을 제거해야 합니다. 그렇지 않으면 FlexConfig 구성이 관리 센터 구성을 덮어씁니다.</p>
클러스터 상태 모니터 대시보드	7.3	<p>이제 클러스터 상태 모니터 대시보드에서 클러스터 상태를 볼 수 있습니다.</p> <p>신규/수정된 화면: 시스템 (⚙️) > Health(상태) > Monitor(모니터)</p>
VMware 및 KVM에서 Threat Defense Virtual에 대해 클러스터링	7.2	<p>threat defense virtual는 VMware 및 KVM에서 최대 4개의 노드에 대한 개별 인터페이스 클러스터링을 지원합니다.</p> <p>신규/수정된 화면:</p> <ul style="list-style-type: none"> • Devices(디바이스) > Device Management(디바이스 관리) > Add Cluster(클러스터 추가) • Devices(디바이스) > Device Management(디바이스 관리) > More(더 보기) 메뉴 • Devices(디바이스) > Device Management(디바이스 관리) > Cluster(클러스터) <p>지원되는 플랫폼: VMware 및 KVM의 Threat Defense Virtual</p>

번역에 관하여

Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.